

Exhibit A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION,

Plaintiff,

v.

MAURA HEALEY, ATTORNEY GENERAL OF
THE COMMONWEALTH OF
MASSACHUSETTS, in her official capacity,

Defendant.

Civil Action No. 1:20-cv-12090

DEFENDANT'S TRIAL AFFIDAVIT OF AARON LOWE

I, Aaron Lowe, declare and say as follows:

I. Background

1. I am the Senior Vice President, Regulatory and Government Affairs at the Auto Care Association (“Auto Care”), a trade group that represents independent automotive “aftermarket” businesses. The “aftermarket” is a term that is used to refer to everything that happens to a vehicle once it leaves the showroom. Aftermarket businesses include repair facilities that perform vehicle service, maintenance, and repair as well as businesses that manufacture, distribute, and sell motor vehicle parts, accessories, tools, equipment, materials, and supplies. Many aftermarket businesses are located or do business in Massachusetts. In this testimony, I will describe my personal knowledge of the history of the 2020 Right to Repair Law, including the 2012 Massachusetts ballot question and the memorandum of understanding entered into by the independent aftermarket and the automotive manufacturers in 2014.

2. The “independent aftermarket” refers to aftermarket businesses and repair facilities that are not affiliated with the original equipment manufacturer, or the “OEM,” such as an independent repair shop.

3. In my current role, I oversee Auto Care’s federal and state legislative and regulatory efforts. This involves advocating for federal and state legislation and rulemaking that protects and benefits our member business. Sometimes it involves testifying before Congress and state legislative bodies in support of or in opposition to pending legislation. I also oversee efforts to work with the OEMs and with other trade organizations to reach agreements on issues important to our member businesses.

4. My work with issues important to the independent aftermarket has spanned decades. I first joined the Automotive Parts and Accessories Association (APAA), a predecessor to the Auto Care Association, in 1982. APAA later merged with another organization to become the Automotive Aftermarket Service Industry Association, which eventually changed its name to the Auto Care Association, where I work today.

5. I have a Bachelor of Arts degree from George Washington University in economics.

II. The Independent Aftermarket

6. Based on my nearly four decades of working on behalf of the aftermarket, I have extensive knowledge of the automobile repair market.

7. Independent repair facilities are a critical part of the automobile repair market. They provide an alternative for vehicle owners who need to service or repair their vehicles and for whom a franchised dealer is cost prohibitive or inconvenient. Many vehicle owners patronize independent repair shops for routine maintenance, and once their vehicle’s warranty expires, the majority of vehicle owners patronize independent repair shops for maintenance and repairs based on price, convenience, and trust.

8. Independent repair shops can provide significant cost savings for vehicle owners. Typically, the third-party parts used by independent repair shops are less expensive than the parts used by manufacturers, and most independent repair shops charge less for labor than dealers. And in the event of a repair requiring a tow, an independent repair shop may be the nearest option for repair.

9. Independent repair shops also can offer greater convenience to vehicle owners, who may live far away from the closest franchised dealer, or who may not be able to get an appointment for a needed service or a repair at a franchised dealer. Many vehicle owners have gained a level of trust with their local independent repair shop and wish to continue to bring their vehicle for service and repair to that shop even as they purchase different makes and models of vehicles over the years.

10. Over the decades I have worked in this industry, I have observed many instances where the OEMs have designed and built their vehicles in ways that make it difficult, and in some instances impossible, for independent repair shops to provide the same services as franchised dealers or to provide the same services as quickly or as efficiently without access to the information, tools, and software only available from the OEM. For example, as I will discuss later in this affidavit, many OEMs require software updates to a vehicle's operating systems in order to complete a repair. Those updates are only available from the OEM.

11. OEMs add design features to their vehicles that require access to mechanical information in order to perform repairs. Sometimes repair procedures are either not available or unreasonably difficult for independent repair facilities to access, thus forcing customers to service their vehicles at franchised dealers, usually at a higher cost, and often at greater inconvenience.

12. As vehicles have become more technically sophisticated, and access to a greater amount of technical information and sophisticated diagnostic capabilities is necessary to service vehicles, the independent repair shops can be at an increasing disadvantage as compared to their dealer counterparts.

13. The current dispute between the OEMs and the aftermarket related to access to on-board diagnostic systems and telematics system data is part of some OEMs' consistent track record, beginning in the 1990s when vehicles began to be equipped with computers, of withholding or making information and tools needed to diagnose and repair late model vehicles too difficult or expensive for independent repair shops to obtain.

14. Auto Care's efforts to level the playing field between independent repair shops and the OEMs' franchised dealers have always met with strong OEM opposition and OEM claims—that have not come to pass—that providing increased access to vehicle information would be an invitation for unscrupulous mechanics to skirt the law and endanger drivers.

III. The Clean Air Act Amendments of 1990 and EPA Regulations

15. The first significant dispute related to vehicle information between the aftermarket and the OEMs that I was involved in was in the 1990s. This dispute related to the Clean Air Act, the Clean Air Act Amendments of 1990, and independent repair shops' ability to access on-board diagnostic ("OBD") systems that Congress was considering requiring on new vehicles. These systems would be used to diagnose issues with vehicles' emissions control systems in order to enable emissions-related maintenance and repairs.

16. In the 1990s, both the federal and California regulations required that OEMs install OBD systems on their vehicles to monitor and detect malfunctions in emissions control systems.

17. As initially proposed by OEMs, access to the required OBD systems would not be standardized. That is, the OBD systems would not be accessible using a standardized tool, but

instead independent repair shops would need to purchase an expensive proprietary tool for every manufacturer, significantly raising the cost for independent repair shops. Allowing this issue to go unchecked likely would have given franchised dealers a monopoly over service of the emissions-related components of vehicles.

18. Auto Care and other aftermarket trade organizations advocated before both houses of Congress during congressional consideration of the Clean Air Act Amendments in favor of requiring that access to the required OBD port be standardized and that any information or tools needed to perform emissions-related repairs be provided to anyone repairing vehicles so that vehicle owners would not be compelled to have all emissions-related service work done at franchised dealers.

19. The OEMs fought the enactment of federal standards. The OEMs argued that allowing independent mechanics access to emissions-system related information would allow unscrupulous mechanics to tamper with vehicles' engines to increase engine performance in a way that would circumvent the vehicle's emissions control systems and violate the Clean Air Act.

20. Ultimately, in 1990, Congress rejected the OEMs' objections and enacted legislation, referred to as the 1990 Clean Air Act Amendments, that required that the connectors for the OBD system be standardized; that access to the OBD port be unrestricted and not require an access code, or use of a device only available to the OEMs; and that the data that comes from the OBD port be usable without the need to further de-code it or use another device to use the information. They also required that OEMs provide independent repair shops the same information they provided their franchised dealers about how to use the emissions-control system and to make emissions-system related diagnosis and repairs

21. The bills passed, and the Clean Air Act was amended to give the aftermarket this critical information necessary to perform maintenance and repair of their customers' vehicles' emissions-related systems. Specifically, 42 U.S.C. § 7521(m)(5) of the Clean Air Act now directs the EPA to require manufacturers to provide to "any person engaged in the repairing or servicing of motor vehicles or motor vehicle engines . . . any and all information needed to make use of the [vehicle's] emission control diagnostic system . . . and such other information including instructions for making emission-related diagnoses and repairs." It further provides that "[n]o such information may be withheld" as a trade secret "if that information is provided (directly or indirectly) by the manufacturer to franchised dealers or other persons engaged in the repair, diagnosing, or servicing of motor vehicles or motor vehicle engines."

22. After the 1990 Clean Air Act Amendments, the Environmental Protection Agency proposed new regulations implementing the "information availability" requirements in the 1990 Clean Air Act Amendments. During the EPA's development of these regulations, the OEMs strongly opposed providing independent repair shops with the ability to update the vehicle software that OEMs often required to complete an emissions-related repair. OEMs claimed in their comments on the proposed rulemaking that access to this capability would lead to independent repair shops tampering with vehicle emissions systems.

23. In 1995, the Environmental Protection Agency issued its regulations (60 Fed. Reg. 40474). Among other means of making information equally available to the aftermarket, the EPA required that OBD systems conform to uniform industry standards and that they be accessible with the use of a standard hand-held diagnostic tool. *See* 40 C.F.R. § 86.1808-01(f)(2)(i) (maintenance instructions requiring that repair shops receive access to "any and all information needed to make use of the on-board diagnostic system and such other information, including instructions for

making emission-related diagnoses and repairs,” and providing that “[n]o information may be withheld . . . if that information is provided (directly or indirectly) by the manufacturer to franchised dealers or other persons engaged in the repair, diagnosing, or servicing of motor vehicles or motor vehicle engines”); 40 C.F.R. § 86.010-38(j)(3)(i) (same).

24. The EPA rejected the OEMs’ objection and by these regulations required that OEMs provide independent repair shops with the ability to update vehicle software.

25. To the best of my knowledge, the harm the OEMs claimed would happen if the OBD ports were standardized and the independent repair facilities had the same access to software updates as the OEMs’ dealers did not come to pass.

IV. Secure Data Release Model

26. Another fight with the OEMs about access to vehicle information was related to immobilizer systems in vehicles. Immobilizer systems are anti-theft systems that prevent a car from starting without an activation or authorization code, which is typically sent to the immobilizer system by the vehicles’ key. These immobilizer systems prevented locksmiths from being able to open vehicle doors for customers without the OEMs’ access code and prevented independent repair shops from performing many repairs, forcing both locksmiths and independent repair shops to send vehicles back to the franchised dealer.

27. The OEMs strongly opposed providing locksmiths or the aftermarket access to key codes. They claimed that doing so would introduce serious security issues, making it easier for thieves to obtain key codes and steal vehicles. However, as a consequence of legislation enacted in the State of California in 2006, OEMs were required to provide the key codes to non-dealers. After that law was enacted, the OEMs and the aftermarket were able to work cooperatively to arrive at a solution that has worked well for both industries.

28. This solution is the Secure Data Release Model (“SDRM”) project and its accompanying VSP Registry. The VSP Registry provides security-related service information, like key codes for immobilizer systems, to security professionals, including repair technicians, who register so that they can securely work on vehicles.

29. Once the SDRM was instituted, the OEMs have been able to work within the system to ensure key codes are available to proper entities, while ensuring that individuals or companies that fail to follow the rules can be tracked and prosecuted if necessary.

V. The History of the 2013 Right to Repair Law and the 2014 Memorandum of Understanding

A. Background

30. Although the 1990 Clean Air Act Amendments and subsequent EPA rulemaking gave the independent aftermarket and franchised dealers equal access to vehicles’ emissions-related systems, it did not necessarily require equal access to information needed to diagnose, repair, and maintain non-emissions-related systems.

31. After the 1990 Clean Air Act Amendments and the 1995 EPA rulemaking, OEMs increasingly connected components of their vehicles to the vehicles’ computer system.

32. However, information related to these other systems was beyond the reach of the 1990 Clean Air Act Amendments and the EPA’s subsequent rulemaking because they were not related to vehicles’ emissions-related systems. Additionally, the requirement that OEMs provide emissions-related information was not consistently enforced by the EPA.

33. As vehicles became more reliant on computers, some OEMs designed their vehicle systems so that they could still be serviced by the aftermarket, but others did not. This caused three key issues related to the information necessary for the diagnosis, maintenance, and repair of vehicles: the information was available, but difficult to access; the information was available, but

priced too high for most independent repair shops to afford it; or the information was not available at all, at any price.

34. The current right to repair effort was born from this increasing reliance by OEMs on computers in their vehicles and their efforts to make it more difficult for independent repair shops to access vehicle information necessary to diagnose, repair, and maintain their customers' vehicles.

B. Federal Right to Repair Bills

35. First, Auto Care advocated for federal legislation to address the problem created by the OEMs' efforts to keep critical information necessary to diagnose, repair, and maintain vehicles from independent repair shops. The Motor Vehicle Owners Right to Repair Act, S. 2617, was first introduced in the Senate in 2001. The purpose of the Act was to make sure that, just as independent repair facilities had access to the information they needed to repair emissions-related systems, they had access to the information they needed to repair the vehicles' other systems as well.

36. In July 2002, I testified in favor of the bill before the Senate Committee on Commerce, Science, and Transportation's Subcommittee on Consumer Affairs, Foreign Commerce and Tourism.

37. In 2005, the aftermarket trade organizations attempted to reach an agreement with the OEMs that would make federal legislation unnecessary. The OEMs' refusal to agree on several key areas derailed the negotiations and any potential agreement. For example, the OEMs would not agree that the tools made available to the independent repair shops would have the same capabilities as those the OEMs provided to their franchised dealers or that similar capabilities be provided to the independent aftermarket at a reasonable cost. Further, we were concerned that any voluntary commitment by the OEMs to make information accessible would not be enforceable if an OEM decided to change its mind.

38. The 2001 bill was revised and re-introduced in the House as the Motor Vehicle Owners' Right to Repair Act of 2005, H.R. 2048. I testified in support of this legislation before the Committee on Energy and Commerce in 2005, and before the House Committee on Small Business in 2008.

39. The OEMs continued to strongly oppose the bill, claiming that the independent aftermarket already had all of the information that they needed to diagnose, repair, and maintain vehicles, and that the bill was an attempt by the independent aftermarket to obtain OEM trade secrets.

40. Ultimately, because of the strenuous opposition of the OEMs to this legislation, Auto Care was unable to make any real headway in this national legislative effort.

C. 2012 Massachusetts Right to Repair Ballot Question and 2013 Right to Repair Law

41. Next, beginning in the early 2010s, the independent aftermarket decided to introduce right to repair legislation at the state level. I helped to coordinate Auto Care's successful 2012 effort to enact right to repair legislation in Massachusetts, a state selected in part because of its strong consumer protection laws.

42. In 2012, Auto Care and other organizations lobbied to pass a right to repair bill in Massachusetts. At the same time, Auto Care collected enough signatures to have the right to repair issue on the ballot as a ballot question as well. In July 2012, the Massachusetts legislature passed H.4362, a compromise version of the bill supported by the aftermarket. However, the aftermarket and the OEMs failed to reach agreement on the compromise legislation before the deadline for removing the right to repair question from the ballot so the initiative appeared on the 2012 ballot.

43. Eighty-six percent of Massachusetts voters voted in favor of the ballot question. The legislature then passed a bill to reconcile the compromise legislation and the ballot question, which was signed into law in 2013 (hereinafter, the “2013 Right to Repair Law”).

D. 2014 Memorandum of Understanding and Right to Repair Agreement

44. On January 15, 2014, after the 2013 Massachusetts Right to Repair bill passed, the Automotive Aftermarket Industry Association (“AAIA”), the Coalition for Auto Repair Equality (“CARE”), the Alliance of Automobile Manufacturers (“Alliance”), and the Association of Global Automakers (“Global Automakers”) entered into a Memorandum of Understanding and Right to Repair Agreement (the “MOU”). A true and accurate copy of the Memorandum of Understanding and Right to Repair Agreement is marked as Exhibit 1 and is attached hereto. The MOU extended the Massachusetts 2013 Right to Repair Law’s requirements nationally. Vehicle manufacturer members of the Alliance and Global Automakers all committed individually to the agreement in all fifty states and in the District of Columbia. For their parts, so long as the OEMs complied with the MOU’s requirements, AAIA and CARE agreed to oppose any additional right to repair legislation until January 2019.

45. The parties also agreed to “work together to resolve any future or related RTR issues that might otherwise be the subject of state legislation,” which could be included in amendments to the MOU by mutual consent of the parties.

46. The parties agreed to meet at least semi-annually to assess how the MOU is operating, and discuss other relevant matters.

47. The MOU required that for model year 2002 vehicles and thereafter, the OEMs would make available for purchase by vehicle owners and independent repair facilities the same diagnostic and repair information, including repair technical updates, that it makes available to its dealers through its internet-based diagnostic and repair information system or other electronically-

accessible manufacturer's repair information system. It also required that OEMs make available for purchase by vehicle owners and independent repair facilities all diagnostic repair tools that the OEMs make available to their dealers.

48. Starting in model year 2018, the MOU requires that OEMs make all of their repair software and operating system updates available from an internet-based diagnostic and repair information system or other electronically-accessible information system, for which independent repair facilities can purchase daily, monthly, or yearly subscriptions at a reasonable cost. In practice, this has required the OEMs to make their repair software and operating system available in the cloud for independent repair shops to download to a laptop. Model year 2018 vehicles were also required to have a non-proprietary interface compliant with industry standards.

49. At that time, telematics was a very new technology. GM was one of few OEMs that had developed a telematics system—the OnStar system that GM still uses today. I know based on my involvement in the negotiations over the 2013 Right to Repair Law and the MOU's terms that GM strongly opposed including telematics system data in the 2013 Right to Repair Law and the MOU, and GM would not agree to the MOU unless it excluded telematics system data. Because telematics was still a new technology and few vehicles were equipped with telematics systems, the aftermarket organizations decided that we would not insist that telematics be included in the MOU and risk the MOU negotiations falling apart. For that reason, the MOU, and the 2013 Right to Repair Law, excluded telematics system information except for telematics system information that is provided to the franchised dealer, necessary for diagnosis and repair, and not otherwise available from the onboard diagnostic system.

50. The MOU includes a dispute resolution mechanism for an independent repair shop that believes an OEM is not in compliance with the MOU. This lengthy process requires the

independent repair shop to first inform the OEM in writing; then wait for a response from the OEM; if the response is unsatisfactory, the independent repair shop must appeal the OEM's decision to a dispute resolution panel created by the MOU, which will attempt to reach agreement and, failing an agreement, issue a decision. If the independent repair facility remains unsatisfied with the resolution of the matter, it may seek legal redress.

E. OEM Compliance Issues

51. Although the 2013 Right to Repair Law was an important step to protect the ability of independent repair shops to diagnose, repair, and maintain their customer's vehicles, there were issues with the OEMs' compliance with the 2013 Right to Repair law and the MOU. I am familiar with these compliance issues because my responsibilities at Auto Care include working with independent repair shops to resolve data access issues.

52. For example, in 2017, Auto Care sent letters to all of the OEMs requesting the status of their compliance with the law's and MOU's requirements for the 2018 model year. While many of the OEMs responded that they would be compliant, Auto Care's subsequent testing of a sample of model year 2018 models confirmed that this was not the case. Mercedes Benz, for example, did not have a subscription service available to independent repair shops; rather, it sent a compact disc to independent repair shops that purchased one, which took an extended period of time for independent repair shops to obtain. Not only was this practice not compliant with the law and the MOU, but it also meant that if an independent repair shop needed that information for a repair of a customer's vehicle, it would not receive it in time to provide any services for that customer—the shop would be forced to recommend the customer get the service at the Mercedes Benz dealer.

53. GM was also not in compliance with this portion of the MOU. GM implemented a subscription system that required technicians to pay per VIN, and thus did not have a daily, yearly, or monthly subscription as required by the 2013 Right to Repair Law or the MOU.

54. Hyundai and Kia did not have any plans to comply with the law until Auto Care pushed them for their plans for compliance.

55. On behalf of Auto Care, I wrote a letter to the National Automotive Service Task Force (“NASTF”) informing it of these issues with the OEMs’ compliance. A true and accurate copy of the letter is marked as Defendant’s Exhibit D and is attached hereto.

56. I am on the Board of Directors of NASTF. NASTF was established in 2000 to identify, communicate, and resolve gaps in the availability and accessibility of automotive service information, service training, diagnostic tools, and equipment for the benefit of automotive service professionals and their customers. NASTF has around 18,000 members.

57. Unfortunately, NASTF has limited authority to resolve the increasingly complex problem of providing independent mechanics with the information they need to service vehicles, and NASTF is often dependent on the OEM’s willingness to resolve the issue. Further, based on the amount of time it takes NASTF to resolve an information accessibility issue raised by an independent repair shop, the independent repair shop sometimes has to refer the affected customer to the franchised dealer to complete the repair while they wait for NASTF’s resolution.

58. As another example, in March 2019, I raised with the Alliance for Automotive Innovation (“Auto Innovators”), another issue with Mercedes Benz’s compliance with the 2013 Right to Repair Law and the MOU. Mercedes Benz was not responding to concerns raised by multiple independent repair shops related to access issues with a Mercedes Benz diagnostic kit. A true and accurate copy of my March 20, 2019, email to Jessica Simmons and Charles Haake at Auto Innovators is marked as Defendant’s Exhibit F and is attached hereto.

59. The independent repair shops seeking to resolve this Mercedes Benz access issue enlisted NASTF's assistance, but NASTF was also unable to get a response from Mercedes Benz. *See* Def.'s Ex. F.

VI. Need for 2020 Right to Repair Law

60. After the 2013 Right to Repair Law passed, more OEMs equipped their vehicles with telematics systems. Telematics systems transmit information about a vehicle to the OEM wirelessly. Including a telematics system on a vehicle permits the OEM to transmit mechanical data needed for diagnosis, repair, and maintenance wirelessly.

61. Equipping their vehicles with telematics systems gave OEMs new ways to control the mechanical data of their customers' cars after selling the cars. It also gave OEMs new ways to limit repair shop access to this information for diagnosis, repair, and maintenance of their customers' vehicles.

62. As a result, OEMs could limit the information available to repair technicians from the OBD system. The 1990 Clean Air Act Amendments only require that OBD systems on vehicles provide emissions-system information. Thus, there is no federal requirement that the OBD system provide direct repair data, such as the repair codes that repair technicians rely on to diagnose and repair vehicles, for non-emissions systems. OEMs could instead route that repair data through the telematics system and have full control over who gets access to that data and on what terms. And for cars with no emissions, like electric vehicles, OEMs do not need to include OBD systems at all under federal law, leaving mechanics unable to repair those vehicles without access to the telematics system data needed for diagnosis, maintenance, or repair.

63. Further, since under the 2013 Right to Repair Law, OEMs are only required to provide the repair information they provide their franchised dealers, car companies like Tesla that do not have franchised dealers and do not equip their vehicles with OBD systems do not need to

comply with either the federal emissions service information regulations or the 2013 Right to Repair Law.

64. Through my work with Auto Care member businesses, I know that since the 2013 Right to Repair Law was enacted, OEMs have made it more difficult for independent repair shops to access information using the OBD port. FCA, for example, began to require that independent mechanics seek authorization through an online portal every time they attempted to use the OBD port for diagnosis or repair. Authorization sessions time out after a certain period of time, meaning that mechanics have to log back in to seek authorization multiple times while working on a single repair. So long as independent repair shops do not have direct access to their customers' vehicles' data, OEMs are able to make it more difficult and expensive for independent repair shops to obtain the data mechanics need to diagnose, repair, and maintain their customers' vehicles. If other OEMs developed similar proprietary portals, independent repair shops would no longer have the standardized access to the OBD port required by the Clean Air Act for non-emissions related information, and it would increase repair costs for consumers.

65. Additionally, the 2013 Right to Repair Law gave OEMs significant discretion to decide what vehicle data independent repair shops should get. Because under that law independent repair shops did not have *direct* access to the information they needed to diagnose, repair, or maintain a vehicle, OEMs were in control of deciding what an independent repair shop would "need" to diagnose, repair, or maintain its customer's vehicle.

66. Additionally, while the 2013 Right to Repair Law requires that OEMs make repair information, tools, and software available to the independent aftermarket, it does not require direct access to the repair codes generated by a vehicle, which are critical to an independent repair shop to diagnose and repair a vehicle. Because OEMs do not need to provide independent repair shops

direct access to repair codes under the 2013 Right to Repair Law, OEMs are able to control how that data is provided to independent repair shops, and on what terms. For example, in Europe, OEMs are pressing regulators to require that independent repair shops only access vehicle data through an OEM-maintained cloud, making the OEM the full gatekeeper for access to in-vehicle diagnostic and repair data for their vehicles.

67. Because of the increasing prevalence of telematics in OEM vehicles, I believed it was important to act on behalf of our business members before the technology advanced any further.

VII. Meetings with OEMs, the Alliance, and Global Automakers about Telematics

68. Beginning in 2015, we repeatedly met with and gave technical presentations to the predecessor organizations to Auto Innovators, the Alliance, and Global Automakers, as well as to individual OEMs, about how they could securely provide telematics system data to independent repair shops. While we had good conversations, ultimately the Alliance and Global Automakers and the OEMs would not work with us on a solution to this issue. That is why, as we were forced to do in the 1990s and again in 2001-2013 in connection with the 2013 Right to Repair Law, we ultimately sought legislation to require the OEMs to provide better access to vehicle data.

69. Shortly after the MOU was signed, on July 23, 2015, I attended a meeting with, among others, the Alliance and Global Automakers to discuss telematics at AAA headquarters in Detroit, Michigan. At this meeting, I raised with these organizations the importance of starting to work together to make telematics data accessible to the aftermarket. The Alliance and Global Automakers claimed that they did not understand what telematics information the aftermarket needed to access.

70. In response, Auto Care started to develop use cases and examples of the types of data the aftermarket would like to be able to access to best service their customers. We provided

these use cases to the Alliance in advance of a meeting to continue the discussion about telematics on October 19, 2015. Even with the use cases, the Alliance and Global Automakers told us they needed more information to move forward with an agreement related to aftermarket access to telematics system data.

71. On February 18, 2016, several aftermarket organizations met with the Alliance and Global Automakers for a “Telematic Data Industry Meeting” at the Alliance’s headquarters. The meeting included the Alliance and Global Automakers and stakeholders from the repair industry. The main purpose of the meeting was to discuss efforts by the repair industry and the OEMs to address cyber security issues related to telematics and the servicing of vehicles by independent repair shops.

72. Around this time, after significant research and discussion, the aftermarket organizations agreed that the Secure Vehicle Interface (“SVI”), a set of technology standards, was a promising method to protect critical vehicle systems yet give independent repair shops the ability to access the telematics system data they needed to diagnose, repair, or maintain their customers’ vehicles.

73. On August 24, 2016, Auto Care met again with the Alliance and Global Automakers to continue to discuss telematics. At that meeting, we shared with the Alliance and Global Automakers our belief that SVI was a viable option for providing standardized and secure wireless access to vehicle networks. On September 6, 2016, we sent a follow-up letter to the Alliance and Global Automakers. A true and accurate copy of the September 6, 2016, letter is marked as Defendant’s Exhibit B and is attached hereto.

74. In November 2016, we had a significant follow-up meeting about telematics in Las Vegas, Nevada. Thirty-six representatives from nine OEMs, including GM and Mercedes Benz,

and nine automotive and aftermarket trade groups gathered for a technical presentation on SVI and how it could be implemented by the OEMs. The purpose of the meeting was to have a technical discussion between experienced technologists from both the aftermarket and the OEMs about the adoption of SVI. A true and accurate copy of the technical presentation aftermarket representatives delivered at this meeting is marked as Defendant's Exhibit C and is attached hereto.

75. Following this meeting, in December 2016, aftermarket associations, the Alliance, and Global Automakers sent a letter to SAE International, an organization that develops automotive engineering standards, about SVI. A true and accurate copy of the December 13, 2016, letter to SAE International is marked as Exhibit 503 and is attached hereto. We asked SAE International to convene a working group of industry engineers to properly investigate the merits of SVI, or other methods, to determine whether they would provide a solution to the problem of providing secure access to vehicle data.

76. SAE did not respond to our letter until September 2017. SAE's letter informed us that they were not aware of any requirements or regulations that required OEMs to provide a wireless vehicle interface. They had not convened a working group or done any additional work on SVI. A true and accurate copy of SAE International's letter is marked as Exhibit 4 and is attached hereto.

77. In January 2019, I and other representatives from Auto Care, CARE, and AutoZone had a meeting with telematics and cybersecurity executives at GM to discuss the issues with access to telematics systems data that the aftermarket was experiencing, and to deliver a technical presentation on SVI.

78. A few weeks later, I sent a follow-up email to Tim Turvey, GM's Vice President of Aftersales and Customer Care who had attended the meeting. He told me that GM was "in the

process of developing our position on the areas of safety, cybersecurity, and consumer privacy,” and that he would get back to us as soon as possible. A true and accurate copy of my email to Tim Turvey is marked as Exhibit 505 and is attached hereto.

79. In March 2019, Bill Hanvey, President and CEO of Auto Care sent a follow-up email to GM to set up a meeting for a technical presentation on SVI. A true and accurate copy of Bill Hanvey’s email is marked as Defendant’s Exhibit G and is attached hereto. However, the meeting never took place, and the communications petered out despite our efforts to keep them going. GM never engaged with the aftermarket in any meaningful way on SVI.

80. In February 2019, Joe Register, Auto Care’s Vice President for Emerging Technology and I delivered yet another presentation about SVI and secure access to telematics data to Global Automakers at their offices. A true and accurate copy of the presentation that I delivered is marked as Defendant’s Exhibit E and is attached hereto.

81. I have no recollection that any of the OEMs or OEM associations I discussed right to repair with ever raised issues about their ability to comply with federal motor vehicle safety standards or the requirements of the Motor Vehicle Safety Act or the Clean Air Act.

VIII. 2020 Ballot Question

82. After we were unable to make any headway with the OEMs or their trade associations related to telematics data access, we started to work on a legislative solution. Bills were introduced in Massachusetts in both 2019 and 2020 requiring OEMs to provide access to telematics data. Both bills required compliance by 2022.

83. I also started to work on including a question on the 2020 ballot in Massachusetts to require that OEMs provide access to telematics data related to diagnosis, repair, and maintenance of vehicles.

84. In August 2019, Auto Care submitted the ballot question to the Attorney General's Office for approval.

85. In September 2019, the Attorney General certified that the ballot question satisfied the requirements of the Massachusetts Constitution for inclusion on the 2020 ballot.

86. In May 2020, Auto Care received a letter from John Bozzella, Auto Innovators' President and CEO, which was addressed to Auto Care's CEO Bill Hanvey, as well as other aftermarket stakeholders who were working together on the Massachusetts ballot question. Citing the COVID-19 pandemic, Bozzella indicated that the OEMs were interested in collaborating on data access issues and, citing the COVID-19 pandemic, asked the aftermarket stakeholders to "cease pursuit of the Massachusetts ballot initiative immediately." A true and accurate copy of the letter from Bozzella is marked as Exhibit 507 and is attached hereto. My reaction to this letter was that it was completely disingenuous and merely an attempt to pressure the aftermarket into dropping the ballot initiative. The aftermarket had been trying for years to get the OEMs to engage with us on data access issues, and they had refused to work with us on implementing SVI or developing a solution to this problem without a legislative requirement. We replied with a letter to Bozzella reminding him that we had been trying to collaborate with the OEMs for years and expressing our interest in working together to reach an agreement so that we could withdraw the ballot question. A true and accurate copy of the letter to Bozzella is marked as Exhibit 508 and is attached hereto.

87. After we submitted the ballot question, I heard that the National Highway Traffic Safety Administration ("NHTSA") was preparing a statement of its position on the ballot question. Auto Care sent a letter to NHTSA asking to have a meeting with them. We scheduled a meeting for July 2020. Only four days before our meeting with NHTSA, NHTSA informed us that they

had already sent a letter to the Massachusetts legislature. Auto Care sent a letter in response to NHTSA's letter disputing technical aspects of the letter.

88. The day after the ballot question was approved by 75% of Massachusetts voters, Auto Care's CEO Bill Hanvey sent a letter to the Auto Innovators President and CEO, explaining that Auto Care had been providing information about SVI to Auto Innovators members and describing SVI as a method of complying with the ballot question. Hanvey offered to make Auto Care's cyber security experts and resources available to Auto Innovators' members to help them expeditiously implement the ballot question's requirements. A true and accurate copy of the November 4, 2020, letter to Bozzella is marked as Exhibit 510 and is attached hereto. Auto Innovators rebuffed our efforts to work with us to implement the law.

89. Although Auto Innovators is seeking to invalidate the new law through this lawsuit, Auto Care is continuing to work on creating a governance model for implementing Section 3 of this law when it goes into effect. As a part of my current role at Auto Care, I am involved in developing the strategy for the governance model. Auto Care's strategy is to include the OEMs as key stakeholders in the governance model.

I declare under the penalty of perjury that the foregoing is true and accurate, this 27th day of May 2021.

/s/ Aaron Lowe
Aaron Lowe
Senior Vice President, Governmental and Regulatory Affairs
Auto Care Association

Exhibit 1



AUTO ALLIANCE
DRIVING INNOVATION®

AAIA®
Automotive Aftermarket
Industry Association

GlobalAutomakers

CARE

MEMORANDUM of UNDERSTANDING

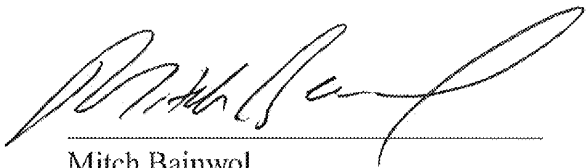
The Automotive Aftermarket Industry Association (“AAIA”), Coalition for Auto Repair Equality (“CARE”), Alliance of Automobile Manufacturers (“Alliance”) and Association of Global Automakers (“Global Automakers”) (“the Original Parties”) enter into this Memorandum of Understanding (MOU) on this Fifteenth (15th) day of January, 2014 and voluntarily agree as follows:

1. The Original Parties fully support this MOU and attached “Right to Repair” (R2R) agreement (“R2R Agreement”). Automobile manufacturer members of the Alliance and Global Automakers indicate their individual company’s agreement to comply with the MOU and R2R Agreement in all fifty (50) States and the District of Columbia through their individual letters of endorsement.
2. Until such time as the provisions of Section 2(c)(i) (common interface device) of the R2R Agreement have been fully implemented, with respect to model year 2018 and newer vehicles, for two years or January 2, 2019, whichever is earlier, and provided the OEMs comply with the MOU during this period, CARE and AAIA agree to continue to work with other Original Parties to fully implement the MOU and to oppose and not to fund or otherwise support, directly or indirectly, any new state R2R legislation.
3. The Original Parties agree to work to strongly encourage any new entrants to the U.S. automotive market or to R2R issues to become signatories to the MOU.
4. The Original Parties agree to work together to resolve any future or related R2R issues that might otherwise be the subject of state legislation and, subject to the mutual consent of the Original parties, amend the MOU and R2R Agreement to include these additional matters.
5. Once the Original Parties have signed on to the MOU, additional parties may join but any amendments or revisions to the terms of the MOU and R2R Agreement, triggered by admission of additional participants, shall require consent of the Original Parties.
6. The Original Parties agree to meet as needed and at least semi-annually, to assess how the MOU is operating, address operational concerns and discuss any other matters relevant to R2R or the MOU or future amendments or parties to the MOU. In the event that one of

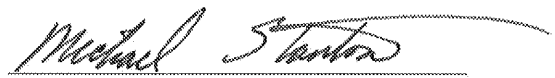
the Original Parties concludes that, due to changed circumstances, the MOU or R2R Agreement may no longer be viable, that party shall, upon thirty (30) days written notice to the other three Original Parties, call a meeting to discuss the need for the MOU and R2R Agreement to continue.

7. The Original Parties agree that should a state(s) pass a law relating to issues covered by this MOU and R2R Agreement, after the effective date of the MOU and R2R Agreement, any automobile manufacturer member of the Alliance and Global Automakers may elect to withdraw its letter of endorsement for the MOU and R2R Agreement partially or entirely for the impacted state(s).

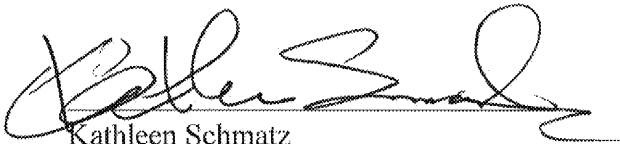
Signed on this 15th day of January, 2014:



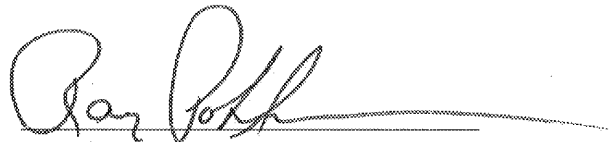
Mitch Bainwol
President & CEO
Alliance of Automobile Manufacturers



Michael Stanton
President & CEO
Association of Global Automakers



Kathleen Schmatz
President & CEO
Automotive Aftermarket Industry Association



Ray Pohlman
President
Coalition for Auto Repair Equality

R2R AGREEMENT

Section 1. As used in this agreement, the following words shall, unless the context clearly indicates otherwise, have the following meanings:

“Dealer”, any person or business who, in the ordinary course of its business, is engaged in the business of selling or leasing new motor vehicles to consumers or other end users pursuant to a franchise agreement and who has obtained a license, as required under applicable law, and is engaged in the diagnosis, service, maintenance or repair of motor vehicles or motor vehicle engines pursuant to said franchise agreement.

“Franchise agreement”, a written arrangement for a definite or indefinite period in which a manufacturer or distributor grants to a motor vehicle dealer a license to use a trade name, service mark or related characteristic and in which there is a community of interest in the marketing of new motor vehicles or services related thereto at wholesale, retail, leasing or otherwise.

“Fair and Reasonable Terms” Provided that nothing in this MOU and R2R Agreement precludes an automaker and an owner or independent repair shop who is subject to the agreement from agreeing to the sale of information and tools on any other terms on which they agree, in determining whether a price is on “fair and reasonable terms,” consideration may be given to relevant factors, including, but not limited to, the following:

(i) The net cost to the manufacturer’s franchised dealerships for similar information obtained from manufacturers, less any discounts, rebates, or other incentive programs.

(ii) The cost to the manufacturer for preparing and distributing the information, excluding any research and development costs incurred in designing and implementing, upgrading or altering the onboard computer and its software or any other vehicle part or component. Amortized capital costs for the preparation and distribution of the information may be included.

(iii) The price charged by other manufacturers for similar information.

(iv) The price charged by manufacturers for similar information prior to the launch of manufacturer web sites.

(v) The ability of aftermarket technicians or shops to afford the information.

(vi) The means by which the information is distributed.

(vii) The extent to which the information is used, which includes the number of users, and frequency, duration, and volume of use.

(viii) Inflation.

“Immobilizer system”, an electronic device designed for the sole purpose of preventing the theft of a motor vehicle by preventing the motor vehicle in which it is installed from starting without the correct activation or authorization code.

"Independent repair facility", a person or business that is not affiliated with a manufacturer or manufacturer's authorized dealer of motor vehicles, which is engaged in the diagnosis, service, maintenance or repair of motor vehicles or motor vehicle engines;

"Manufacturer", any person or business engaged in the business of manufacturing or assembling new motor vehicles.

"Dispute Resolution Panel (DRP)", a 5-person panel established by the Original Parties comprised of the following: one Alliance representative, Alliance member or Alliance designee, one Global Automakers representative, Global Automakers' manufacturer member or Global Automakers designee, two representatives of the independent vehicle repair industry to be selected and mutually agreed upon by AAIA and CARE, and one DRP Chair. The DRP Chair shall be an independent professional mediator with no affiliation to any of the Original Parties, shall be selected by unanimous consent of the Original Parties and shall be funded in equal amounts by each of the Original Parties. The Original Parties shall, at one of the two annual meetings, have an opportunity to revisit their respective representative or ask the Original Parties to revisit the person acting as DRP Chair.

"Motor vehicle", any vehicle that is designed for transporting persons or property on a street or highway and that is certified by the manufacturer under all applicable federal safety and emissions standards and requirements for distribution and sale in the United States, but excluding (i) a motorcycle; (ii) a vehicle with a gross vehicle weight over 14,000 pounds; or (iii) a recreational vehicle or an auto home equipped for habitation.

"Owner", a person or business who owns or leases a registered motor vehicle.

"Trade secret", anything, tangible or intangible or electronically stored or kept, which constitutes, represents, evidences or records intellectual property including secret or confidentially held designs, processes, procedures, formulas, inventions, or improvements, or secret or confidentially held scientific, technical, merchandising, production, financial, business or management information, or anything within the definition of 18 U.S.C. § 1839(3).

Section 2.

(2)(a). Except as provided in subsection (2)(e), for Model Year 2002 motor vehicles and thereafter, a manufacturer of motor vehicles sold in United States shall make available for purchase by owners of motor vehicles manufactured by such manufacturer and by independent repair facilities the same diagnostic and repair information, including repair technical updates, that such manufacturer makes available to its dealers through the manufacturer's internet-based diagnostic and repair information system or other electronically accessible manufacturer's repair information system. All content in any such manufacturer's repair information system shall be made available to owners and to independent repair facilities in the same form and manner and to the same extent as is made available to dealers utilizing such diagnostic and repair information system. Each manufacturer shall provide access to such manufacturer's diagnostic and repair information system for purchase by owners and independent repair facilities on a daily, monthly and yearly subscription basis and upon fair and reasonable terms.

(2)(b)(i) For Model Year 2002 motor vehicles and thereafter, each manufacturer of motor vehicles sold in the United States shall make available for purchase by owners and independent repair facilities all diagnostic repair tools incorporating the same diagnostic, repair and wireless capabilities that such manufacturer makes available to its dealers. Such tools shall incorporate the same functional repair capabilities that such manufacturer makes available to dealers. Each manufacturer shall offer such tools for sale to owners and to independent repair facilities upon fair and reasonable terms.

(ii) Each manufacturer shall provide diagnostic repair information to each aftermarket scan tool company and each third party service information provider with whom the manufacturer has appropriate licensing, contractual or confidentiality agreements for the sole purpose of building aftermarket diagnostic tools and third party service information publications and systems. Once a manufacturer makes such information available pursuant to this section, the manufacturer will have fully satisfied its obligations under this section and thereafter not be responsible for the content and functionality of aftermarket diagnostic tools or service information systems.

(2)(c)(i) Commencing in Model Year 2018, except as provided in subsection (2)(e), manufacturers of motor vehicles sold in the United States shall provide access to their onboard diagnostic and repair information system, as required under this section, using an off-the-shelf personal computer with sufficient memory, processor speed, connectivity and other capabilities as specified by the vehicle manufacturer and:

(a) a non-proprietary vehicle interface device that complies with the Society of Automotive Engineers SAE J2534, the International Standards Organizations ISO 22900 or any successor to SAE J2534 or ISO 22900 as may be accepted or published by the Society of Automotive Engineers or the International Standards Organizations; or,

(b) an on-board diagnostic and repair information system integrated and entirely self-contained within the vehicle including, but not limited to, service information systems integrated into an onboard display, or

(c) a system that provides direct access to on-board diagnostic and repair information through a non-proprietary vehicle interface such as Ethernet, Universal Serial Bus or Digital Versatile Disc. Each manufacturer shall provide access to the same on-board diagnostic and repair information available to their dealers, including technical updates to such on-board systems, through such non-proprietary interfaces as referenced in this paragraph. Nothing in this agreement shall be construed to require a dealer to use the non-proprietary vehicle interface (i.e., SAE J2534 or ISO 22900 vehicle interface device) specified in this subsection, nor shall this agreement be construed to prohibit a manufacturer from developing a proprietary vehicle diagnostic and reprogramming device, provided that the manufacturer also complies with Section 2(c)(i) and the manufacturer also makes this device available to independent repair facilities upon fair and reasonable terms, and otherwise complies with Section 2(a).

(2)(c)(ii) No manufacturer shall be prohibited from making proprietary tools available to dealers if such tools are for a specific specialized diagnostic or repair procedure developed for

the sole purpose of a customer service campaign meeting the requirements set out in 49 CFR 579.5, or performance of a specific technical service bulletin or recall after the vehicle was produced, and where original vehicle design was not originally intended for direct interface through the non-proprietary interface set out in (2)(c)(i). Provision of such proprietary tools under this paragraph shall not constitute a violation of this agreement even if such tools provide functions not available through the interface set forth in (2)(c)(i), provided such proprietary tools are also available to the aftermarket upon fair and reasonable terms. Nothing in this subsection (2)(c)(ii) authorizes manufacturers to exclusively develop proprietary tools, without a non-proprietary equivalent as set forth in (2)(c)(i), for diagnostic or repair procedures that fall outside the provisions of (2)(c)(ii) or to otherwise operate in a manner inconsistent with the requirements of (2)(c)(i).

(2)(d) Manufacturers of motor vehicles sold in the United States may exclude diagnostic, service and repair information necessary to reset an immobilizer system or security-related electronic modules from information provided to owners and independent repair facilities. If excluded under this paragraph, the information necessary to reset an immobilizer system or security-related electronic modules shall be obtained by owners and independent repair facilities through the secure data release model system as currently used by the National Automotive Service Task Force or other known, reliable and accepted systems.

(2)(e) With the exception of telematics diagnostic and repair information that is provided to dealers, necessary to diagnose and repair a customer's vehicle, and not otherwise available to an independent repair facility via the tools specified in 2(c)(i) above, nothing in this agreement shall apply to telematics services or any other remote or information service, diagnostic or otherwise, delivered to or derived from the vehicle by mobile communications; provided, however, that nothing in this agreement shall be construed to abrogate a telematics services or other contract that exists between a manufacturer or service provider, a motor vehicle owner, and/or a dealer. For purposes of this agreement, telematics services include but are not limited to automatic airbag deployment and crash notification, remote diagnostics, navigation, stolen vehicle location, remote door unlock, transmitting emergency and vehicle location information to public safety answering points as well as any other service integrating vehicle location technology and wireless communications. Nothing in this agreement shall require a manufacturer or a dealer to disclose to any person the identity of existing customers or customer lists.

Section 3. Nothing in this agreement shall be construed to require a manufacturer to divulge a trade secret.

Section 4. Notwithstanding any general or special law or any rule or regulation to the contrary, no provision in this agreement shall be read, interpreted or construed to abrogate, interfere with, contradict or alter the terms of any franchise agreement executed and in force between a dealer and a manufacturer including, but not limited to, the performance or provision of warranty or recall repair work by a dealer on behalf of a manufacturer pursuant to such franchise agreement.

Section 5. Nothing in this agreement shall be construed to require manufacturers or dealers to provide an owner or independent repair facility access to non-diagnostic and repair information

provided by a manufacturer to a dealer, or by a dealer to a manufacturer pursuant to the terms of a franchise agreement.

Section 6. If an independent repair facility or owner believes that a manufacturer has failed to provide the information or tool required by this MOU, he may challenge the manufacturer's actions by first notifying the manufacturer in writing. The manufacturer has thirty (30) days from the time it receives the reasonably clear and specific complaint to cure the failure, unless the parties otherwise agree. If the complainant is not satisfied, he has thirty (30) days to appeal the manufacturer's decision to the DRP. The DRP shall be convened by the Chair within thirty (30) days of receipt of the appeal of the manufacturer's decision. The DRP will attempt to reach agreement between the parties. If unsuccessful, the DRP shall convene and issue its decision. The decision must be issued within 30 days of receipt of the appeal of the manufacturer's decision, unless otherwise agreed to by the parties. The DRP decision shall be disseminated to the complainant, the manufacturer, and the Original Parties. If the manufacturer and complainant still cannot reach agreement, the complainant may take whatever legal measures are available to it.

Defendant's Exhibit D



Mr. Donny Seyfer
National Automotive Service Task Force
4501 Harlan St.
Wheat Ridge, CO 80033

Dear Donny,

The Motor Vehicle Owners' Right to Repair Act, enacted in the Commonwealth of Massachusetts in 2013, requires vehicle manufacturers to provide independent repair shops with access at a fair and reasonable cost to the same repair information, tools and software for model year 2002 and later vehicles already provided to franchised new car dealers. Subsequently, the law was the subject of a Memorandum of Understanding (MOU) whereby the vehicle manufacturers agreed to abide by the Massachusetts Right to Repair law nationwide.

With the introduction of the new 2018 model year vehicles, manufacturers are now required to make all of their repair software and operating system updates available over a "manufacturer's internet-based diagnostic and repair information system or other electronically accessible manufacturers repair information system." The MY 2018 provision also mandates that shops be able to download software from the cloud and access the vehicle using a nonproprietary interface that is compliant with either the SAE J25234 or ISO 22900 industry standards. Manufacturers must offer subscriptions to independent shops on a daily, monthly or yearly basis. Under the model year 2018 requirements, a shop would have the ability to download all repair software and operating system updates from a manufacturer's site and then have the same repair and diagnostic capabilities as provided by proprietary dealer tools.

As you are aware, in 2017, the Auto Care Association and the Coalition for Auto Repair Equality (CARE) sent letters to your members requesting an update on their plans to comply with the model year 2018 requirements. Nearly all manufacturers replied that they would be in full compliance with the requirements. However, in March 2018, CARE and Auto Care found during compliance testing of nine model year 2018 vehicles that only three of your members were in full compliance. The remaining six had issues with either their system or the subscription plans being offered. We are in the process of testing five other manufacturers to determine whether they are in compliance.

I have attached the results of the tests that were completed, but below is a summary of what we found:

- **Ford, Toyota and FCA** appear to be in full compliance.
- **Hyundai and Kia** do not have any system in place to meet the MY 2018 requirements (we understand that a request has already been submitted to NASTF on this issue and we are still awaiting a full response).
- **Mercedes** does not provide a daily or monthly subscription. Also, Mercedes requires that technicians purchase a disc which takes an extended amount of time to obtain and therefore violates the letter and the spirit of the law's requirements that the information be housed on an Internet or electronically-based system.
- **Nissan** does not permit daily, monthly or yearly subscriptions as required by the MOU.

- **Volvo** complies for many of its makes but the XC 90 requires a proprietary cable for its interface and therefore does not comply with the requirement that the interface meet either the SAE or ISO standardized interface requirements
- **GM** complied at the time of testing; however, they have recently implemented a new subscription system for reprogramming that requires technicians to pay per VIN and therefore does not have a daily, monthly or yearly subscription system as required by the law and the MOU.

Under terms of the MOU and Massachusetts law, we are requesting that NASTF forward the issues outlined in this letter to the appropriate manufacturers in order to secure a response. We expect that the manufacturers would respond in the appropriate 30-day window required by the MOU and Massachusetts statute.

Thank you in advance for your attention to this very important matter.

Sincerely,

A handwritten signature in black ink, reading "Aaron Lowe". The signature is fluid and cursive, with the first name "Aaron" written in a larger, more prominent script than the last name "Lowe".

Aaron Lowe,
Senior Vice President, Regulatory and Government Affairs
Auto Care Association

A handwritten signature in black ink, reading "Ray Pohlman". The signature is fluid and cursive, with the first name "Ray" written in a larger, more prominent script than the last name "Pohlman".

Ray Pohlman
President
Coalition for Auto Repair Equality (CARE)

Defendant's Exhibit F

Message

From: Aaron Lowe [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=A60E42C207C24F2AAD8CDD98EE23871A-AARON.LOWE]
Sent: 3/20/2019 6:43:34 PM
To: Jessica Simmons [JSimmons@autoalliance.org]; Charles Haake [chaake@globalautomakers.org]
CC: Pohlman, Ray [ray.pohlman@autozone.com]
Subject: RE: Right to Repair DRP

Thanks Jessica, but from what I am hearing, these are only two of many shops that have been waiting on a response from Mercedes on this issue. We really would like to understand why Mercedes continues to drag its feet on responding to issues that arise regarding access to their information. In order to prevent DRP's from becoming a regular occurrence with Mercedes, perhaps we can hold a call with the company, NASTF and our groups to see if we can obtain a more positive attitude from the company to the independents?

AARON LOWE

Senior Vice President, Regulatory & Government Affairs
 Liaison, Upholstery and Trim International Council(UTIC)

Auto Care Association

7101 Wisconsin Ave., Suite 1300
 Bethesda, MD 20814
 Desk: 240-333-1021
 aaron.lowe@autocare.org
 www.autocare.org



Get key stats on the state of the industry and what your association is doing for you. Read the new **State of the Auto Care 2019** report: [autocare.org](#)

This email message is privileged and confidential. If you are not the intended recipient, please delete this message and notify the sender. Any views or opinions

From: Jessica Simmons <JSimmons@autoalliance.org>
Sent: Wednesday, March 20, 2019 2:37 PM
To: Aaron Lowe <aaron.lowe@autocare.org>; Charles Haake <chaake@globalautomakers.org>
Subject: RE: Right to Repair DRP

Aaron,
 Thanks for your email. I have forwarded it to the appropriate people at Mercedes Benz. The two independents should expect a response from Mercedes directly.
 Jessica

From: Aaron Lowe <aaron.lowe@autocare.org>
Sent: Thursday, March 14, 2019 4:47 PM
To: Ellen Gleberman <egleberman@globalautomakers.org>; Jessica Simmons <JSimmons@autoalliance.org>
Subject: Right to Repair DRP

Ellen and Jessica

Pursuant to Section 6 of the Right to Repair Memorandum of Understanding, I have received a request from two repair shops to initiate a Dispute Resolution Panel to address an issue that is occurring between the shop and Mercedes Benz all relating to access to the "XEntry Kit". I have attached the email received from this shop making the request, along with other emails that I have received from other shops regarding the same issue. I further understand from Donny Seyfer at NASTF has attempted to work with Mercedes to obtain the needed information, but have been able to obtain any response. Therefore, under the terms of the Right to Repair MOU, these shops are requesting a dispute resolution panel.

I would propose that we hold a conference call at noon (eastern time) on March 20 to discuss how to address this ongoing issue. Please let me know if all of you would be available for the call or if you have other thoughts on how to proceed on this.

Thanks.

AARON LOWE

Senior Vice President, Regulatory & Government Affairs
Liaison, Upholstery and Trim International Council(UTIC)

Auto Care Association

7101 Wisconsin Ave., Suite 1300
Bethesda, MD 20814
Desk: 240-333-1021
aaron.lowe@autocare.org
www.autocare.org

Get key stats on the state of the industry and what your association is doing for you. Read the new **State of the Auto Care 2019** report: [autocare.org](#)

This email message is privileged and confidential. If you are not the intended recipient, please delete this message and notify the sender. Any views or opinions

Defendant's Exhibit B

September 6, 2016

TO: Alliance for Automobile Manufacturers and Association of Global Automakers

FR: AAA, Auto Care Association, Automotive Aftermarket Suppliers Association, Automotive Service Association, Equipment and Tool Institute and AIA Canada

RE: Follow-up from August 24 Meeting

Vehicles are rapidly evolving from predominately mechanical devices to hybrid designs consisting of multiple inter-connected networks of electronic sensors and controllers designed to optimize vehicle operation and performance. Intelligent Transportation System requirements expands these internal internetworking concepts to include connectivity with other vehicles, city infrastructure and hand-held nomadic devices. It's becoming increasingly clear that the demand for operational vehicle data will increase to serve a variety of infrastructural and commercial requirements as this evolution continues.

It's agreed that Aftermarket devices connecting a vehicle OBDII port using inherently unsecure wireless technologies such as Bluetooth has the potential to offer an easily exploited point of entry for unauthorized access to vehicle networks. In contrast, a single, standardized and secure interface can eliminate this threat while offering a minimal attack surface to intruders. Ideally the same interface will provision access using a physical OBDII connection, as well as secured wireless technologies.

After extensive research and discussion, our group of leading associations representing the aftermarket and motorists agree the ISO Secure Vehicle Interface (SVI) provides a viable option for implementing a standardized and secure access to vehicle networks. The design is based on a set of existing technology standards, defined by recognized Standards Developing Organizations (SDO), including the International Organization for Standardization (ISO), Society of Automotive Engineers (SAE), German Institute for Standardization (DIN), and others. SVI is the latest evolution of the ISO Vehicle Station Gateway, which is further enhanced by three inflight projects under ISO Technical Committee TC-204 Intelligent Transport Systems:

- Secure Vehicle Interface - ISO/AWI TS 21177
- Data Dictionary - ISO/AWI TS 21184
- Communication Profiles - ISO/AWI 21185

At the close of our recent meeting with your groups, we agreed to hold a second meeting to discuss technical merits and concerns with the adoption of SVI by automakers and aftermarket manufacturers. We further agreed that members attending this meeting should include technologists experienced in ITS concepts and requirements, as well as those with an understanding of vehicle diagnostic information currently delivered using the vehicle OBDII port. We also agreed this discussion will focus on a data agnostic technical solution, leaving the

determination as to the data content that would be available from the SVI for a later discussion. Participants unfamiliar with the ISO Vehicle Station Gateway are invited to consult the following list of technical papers used in a practical implementation of this design on behalf of the German military.

ISO 7498-1	ISO 22901 (all parts)	SAE J2186
ISO 13184-2	ISO/IEC 10731:1994	VG 95287
ISO 13185-2	ISO 27145	VG 95916
ISO 13209 (all parts)	DIN EN 61508	SAE J2186
ISO 13400-4	SAE J1930-DA	VG 95287
ISO 14229	SAE J1979-DA	VG 95916
ISO 15031-3	SAE J2013-DA	

Thank you in advance for your efforts to help put this meeting together. We look forward to further discussing our proposed solution with the appropriate technologists representing automakers as soon as practically possible.

Defendant's Exhibit C

ITS Secure Vehicle Interface

November 3, 2016

CONFIDENTIAL

AAI-ACA-0022333

Before We Begin...

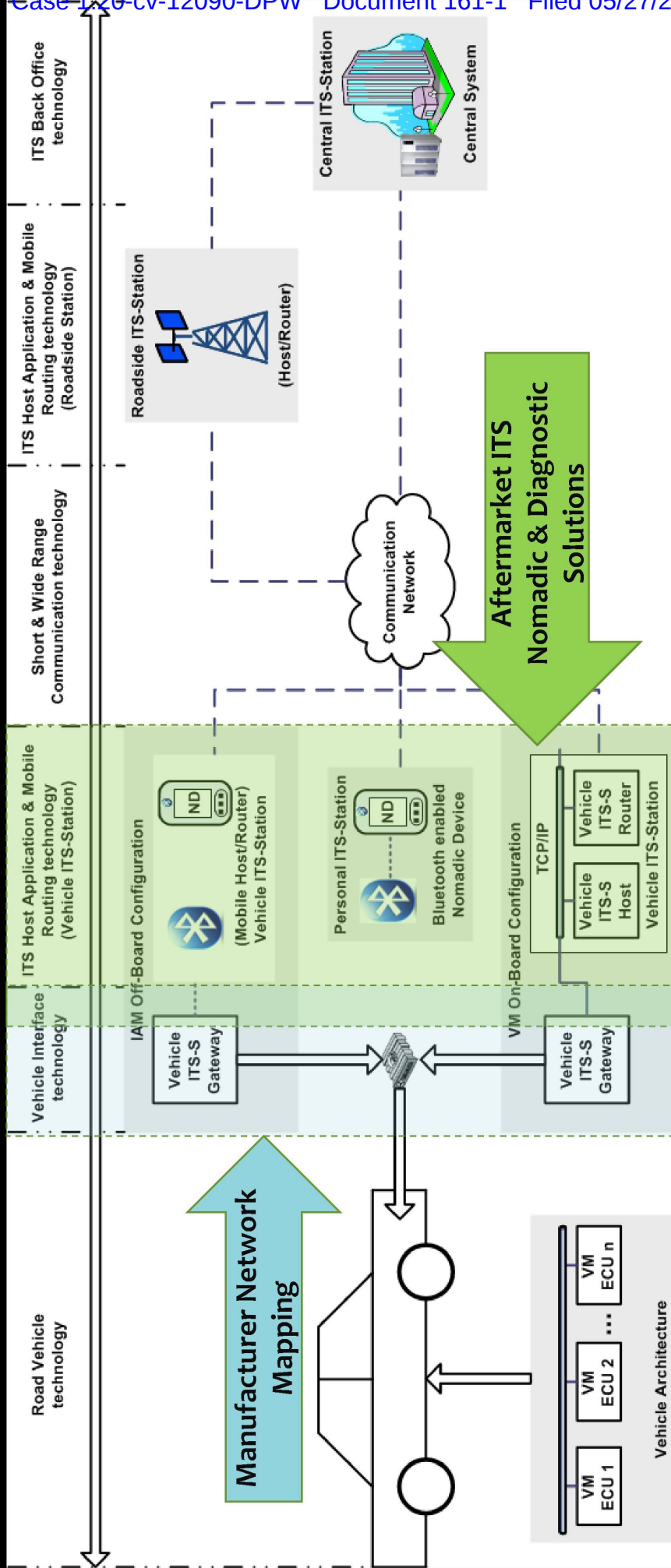
While SVI foundational concepts were referenced using several names over the years, the design objectives and fundamental architecture remained consistent.

- ISO Vehicle Station Gateway (VSG)
- ISO Secure Vehicle Interface (SVI)
- SAE Vehicle Interface Methodology (VIM)

SVI is a software solution that can be implemented in...

- new vehicles by a vehicle manufacturer
- used vehicles through a device attached to the OBDII port

ITS Technology Chain



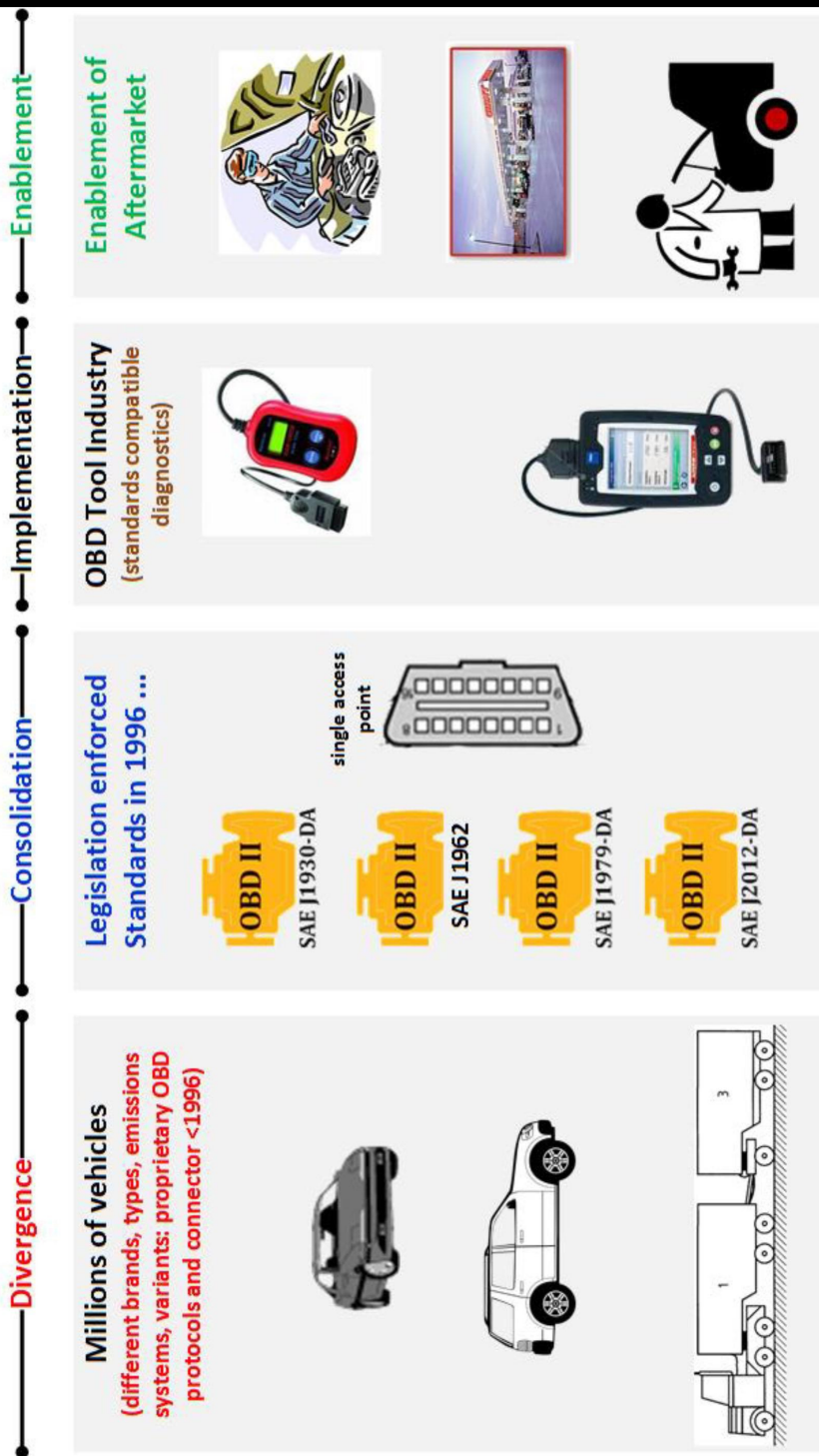
Evolution of OBDII Port

From inception to the recommended future state

CONFIDENTIAL

AAI-ACA-0022336

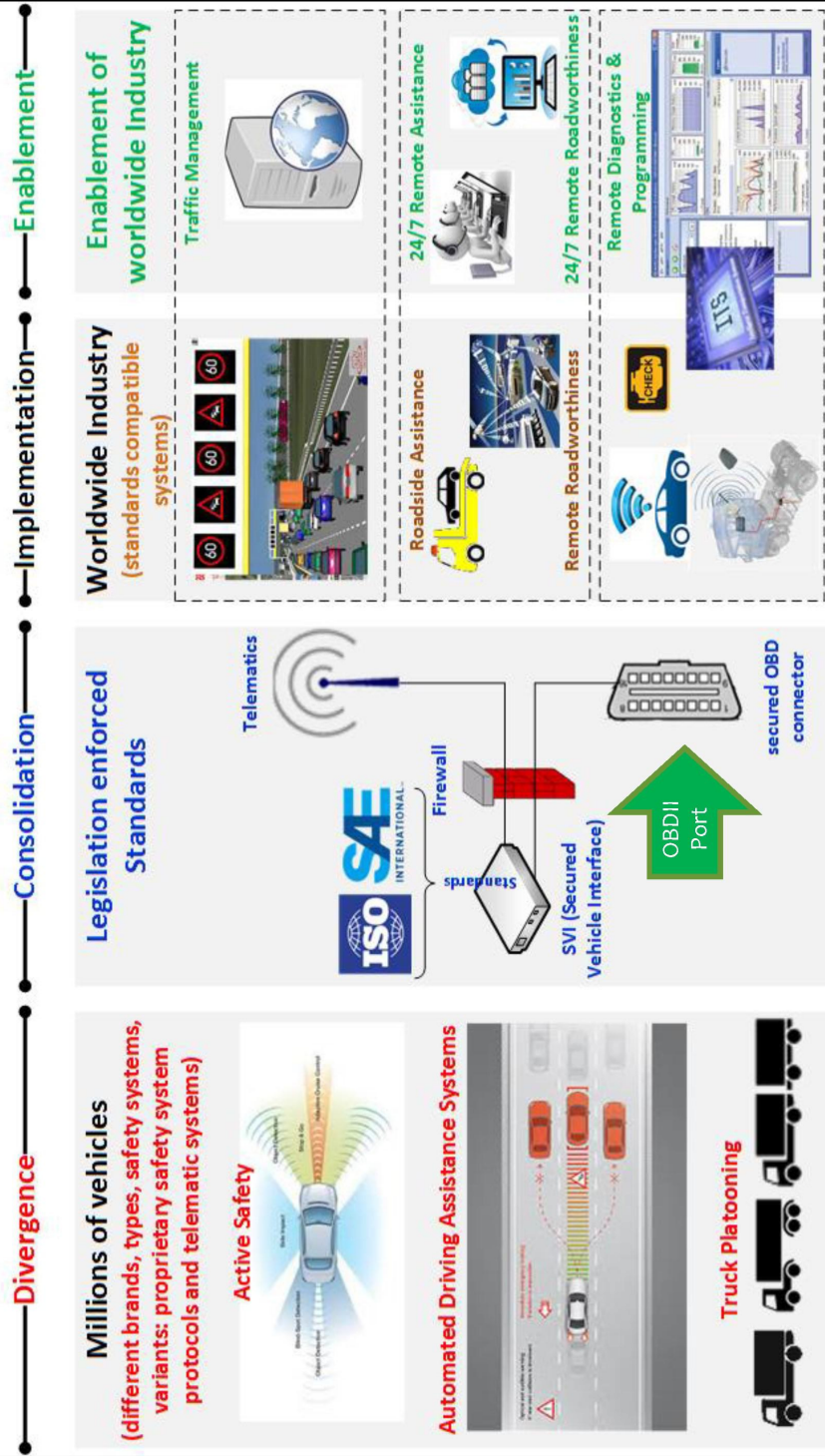
Introduction-OBDI Diagnostic Port



CONFIDENTIAL

AAI-ACA-0022337

Future State – an ITS Compliant Version



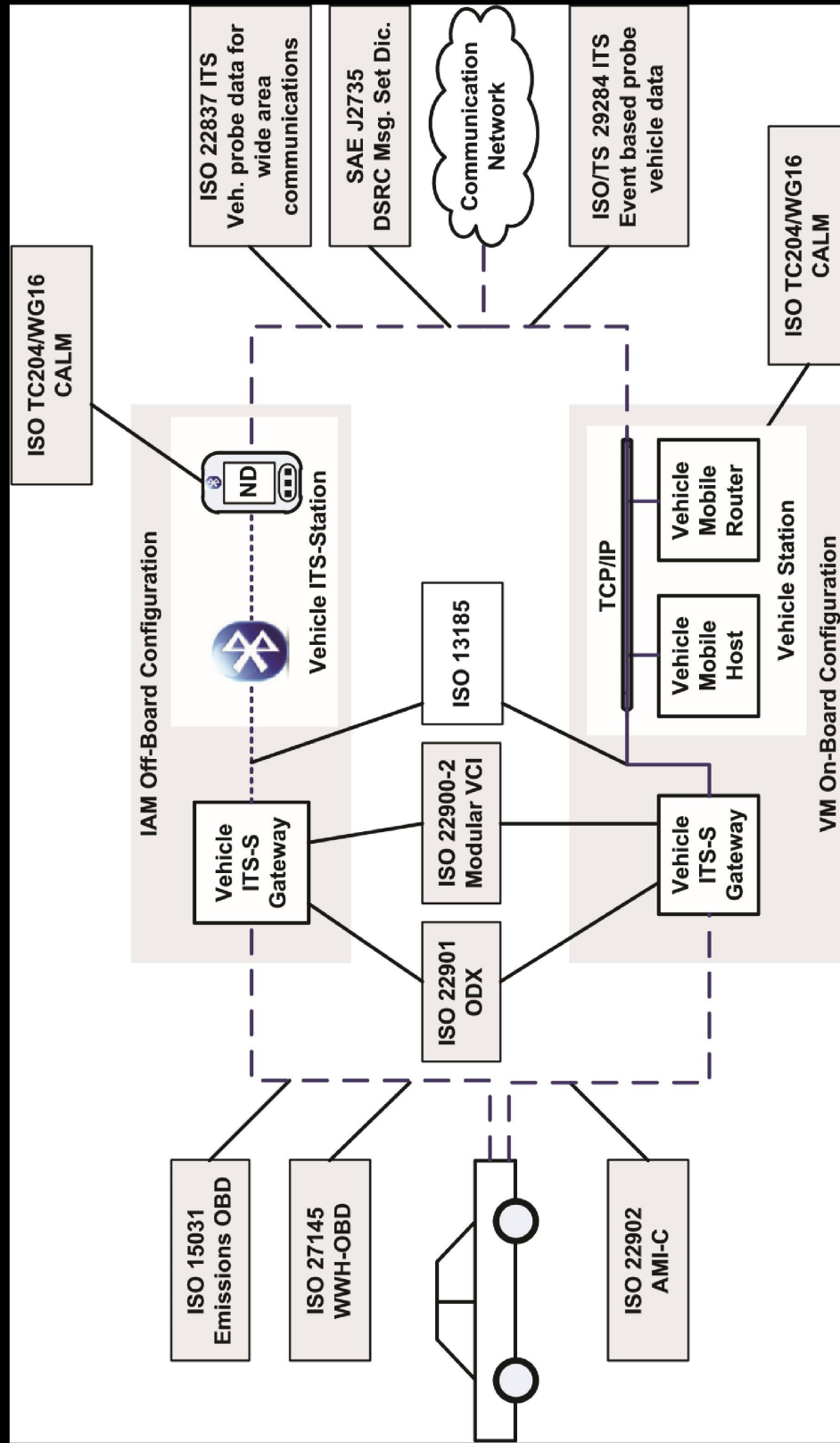
SVI Design Fundamentals



CONFIDENTIAL

AAI-ACA-0022339

SVI / CALM Applicable International Standards



ISO SVI - Also Known as the SAE
Vehicle Interface Methodology



CONFIDENTIAL

AAI-ACA-0022341

Secure Access is Crucial!

Review of ISO WIP to secure SVI communication

CONFIDENTIAL

AAI-ACA-0022342

Issues and Recommendations

Vehicles are cyber-physical systems which must be protected from cyber attack. The default approach is recognized Identity Access Management (IAM) best practices

Credentials used to access vehicle networks issued and governed by independent third parties based on standardized protocols and policies.

Strategies to secure vehicle networks should include the OBDII port, since an unsecure OBDII device “dongle” offers intruders an easily exploited attack surface.

Ideally once interface and firewall is used to protect both physical and wireless connectivity

Internal network controllers are accessed using a standardized set of metadata definitions and a single query strategy.

U.S. DOT issues Federal guidance to the automotive industry for improving motor vehicle cybersecurity

October 24, 2016

CONFIDENTIAL

AAI-ACA-0022344

Secure Wireless Communication

CONFIDENTIAL

AAI-ACA-0022345

New ISO V2X Security Projects

The following projects are designed to strengthen SVI V2X security. These were introduced at the ISO Spring 2016 TC204 WG17 meeting in Potsdam and approved during the Fall 2016 TC-204 WG17 meeting in Concord. Subsequently they were reassigned to TC204 WG18.

Secure vehicle interface - ISO/AWI TS 21177

ITS-station security services for secure session establishment and authentication

Communication Profiles – ISO/AWI 21185

Communication profiles for secure connection between an ITS-station and a vehicle

Security Scope – ISO 21177

The Secure Vehicle Interface (SVI) is a set of functional components that locally connect a vehicle ITS station (V-ITS-S) to a vehicle in a secure manner with minimal latency.

This international standard contains specifications for a set of security services required to ensure the authenticity and integrity of information exchanged between a vehicle and a V-ITS-S.

These services include authentication and secure session establishment which are required to exchange information between a vehicle and a V-ITS-S in a trusted and secure manner.

These services are essential for many C-ITS applications and services including time-critical safety applications and automated driving.

Communication Profiles – ISO 21185

The Secure Vehicle Interface (SVI) is a set of functional components that locally connect a vehicle ITS station (V-ITS-S) to a vehicle in a secure manner with minimum latency.

This international standard contains specifications for the use of existing ISO standardized communication protocols to connect an ITS-station to a vehicle enabling secure low-latency information exchange.

Such exchanges are essential for many C-ITS applications and services including time-critical safety applications and automated driving.

Secure Vehicle Diagnostics

CONFIDENTIAL

AAI-ACA-0022349

Report to WG2 of the ISO TC22/SC31/WG2 Project Team on Authentication, Authorization, and Secure Diagnostic Communication

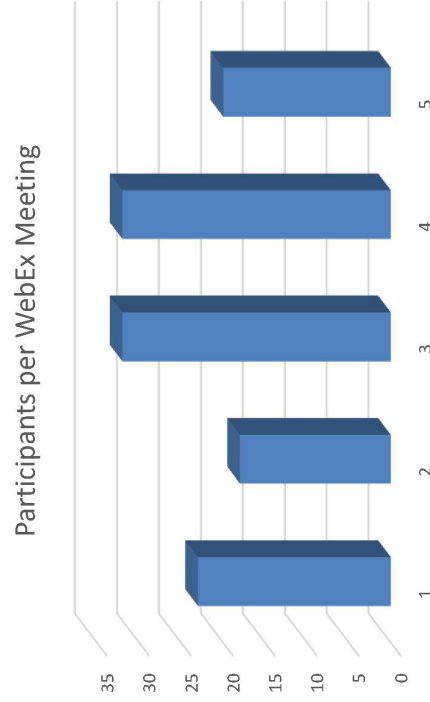
September 1st, 2016
Bernd Gottschalk, Daimler AG
Mark Zachos, SAE

CONFIDENTIAL

AAI-ACA-0022350

- Statistics
- Overview on the WebEx meetings
- Results and recommendations
 - Overview
 - Authentication: History and proposal
 - Secure Communication: Variants for implementation
- Final Statements

- **6 WebEx Meetings** have been hold
- **Average of 25 Participants** per WebEx:



- **35 pages** of UDS draft have been created



International
Organization for
Standardization

More Statistics - Project Team Members

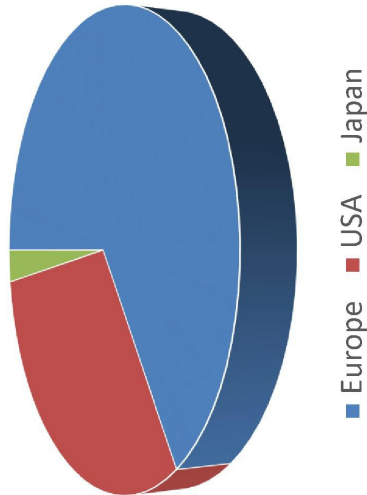
Tony Malaterre	Actia	Mike Westra	Ford
Jacques Kunegel	Actia	Xin Ye	Ford
Andreas Sadler	Audi	Henry Ubik	Ford
Maik Schmidt	BMW	Dirk Pillau	FSD
Robert Rohr	BMW	Tim Proctor	GM
Richard Wimmer	BMW	Brian Grishkevich	Intrepid CS
Marco Le Brun	Bosch	Hiroshi Ninomiya	Mazda, JSAE
Tom Bertosa	Bosch	Francois Rochette	PSA
Mauro Cerrato	CNH Industrial	Georges Emmanuel	PSA
Gangolf Feiter	CSC	Moulay Abdelaziz El Aabid	PSA
Bernd Gottschalk	Daimler	Francois Croc	PSA
Manuel Henle	Daimler	Denis Dessertenne	Renault
Dennis Artz	Daimler	Jean-Baptiste Mangé	Renault
Eric Wern	DIN, VDA	Mark Zachos	SAE, DGTechnologies
Greg Potter	ETI	Robert Hoevenaar	Snap-on
Jin Savich	Fiat Chrysler Automotive	Kevin Harnett	US DOT
Jason Miller	Ford	Oliver Garnatz	Vector
Dave Bardelski	Ford	Jeff Craig	Vector
Bill Waldeck	Ford	Markus Zblewski	Volkswagen
John Turner	Ford	Joakim Pauli	Volvo Trucks

CONFIDENTIAL

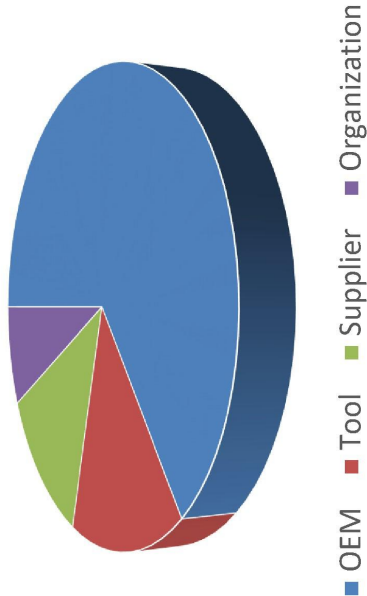
AAI-ACA-0022353

Even more Statistics...

Members by Continent



Stakeholder Groups



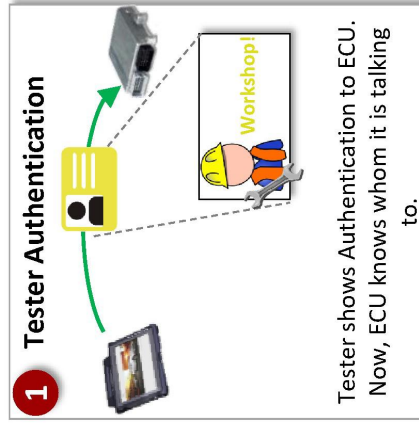
Main discussion points were

WebEx...

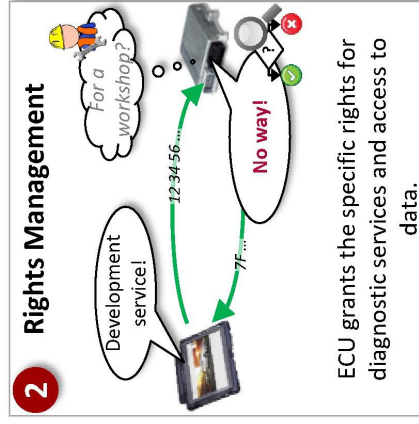
- #1 Overview on the topic
- #2 Variants for Authentication
- #3 Variants for Secure Diagnostic Communication
- #4 New UDS Service „Authentication“
- #5 Feedback and enhancement of UDS Service „Authentication“
- #6 Wrap-up and report to WG2

Overview on the topic

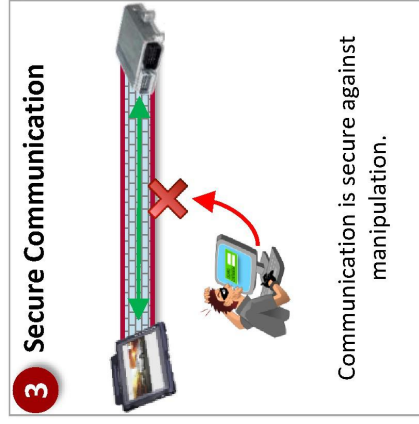
Secure Diagnosis has three main components:



... is the base for Rights
Management and Secure
Communication.



... is the base for controlling
access rights.



... is the base for a secure
rights management.

Daimler:

- Basic principles / overview
- Detailed rights management, but complex
- Partially Tester online approach

Renault:

- Complete lock/unlock of the diagnostic session
- Central online server approach
- Trusted third party server

FCA

- Migration concept (mixed architecture)
- Tester Online approach

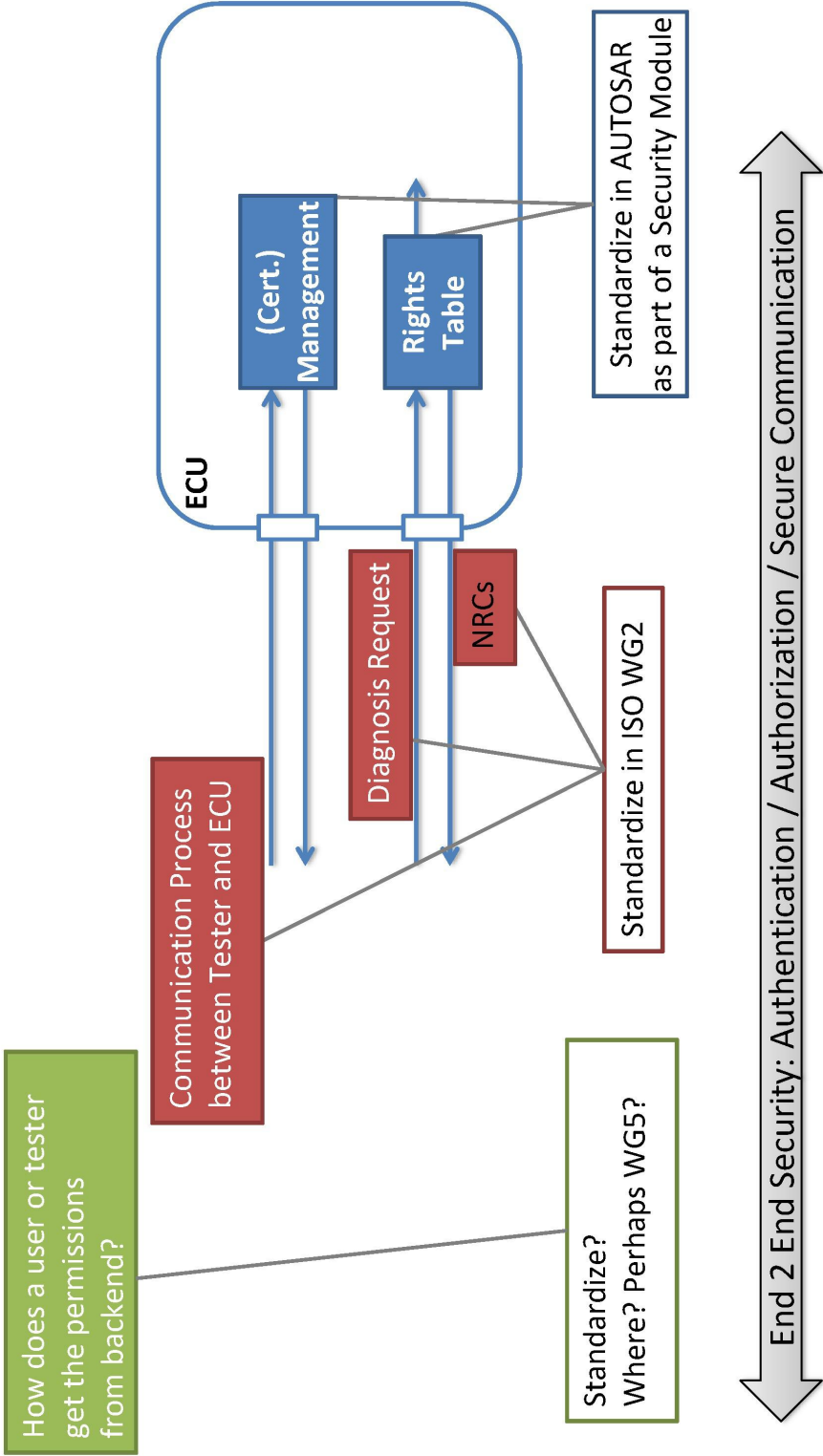
CONFIDENTIAL

AAI-ACA-0022357

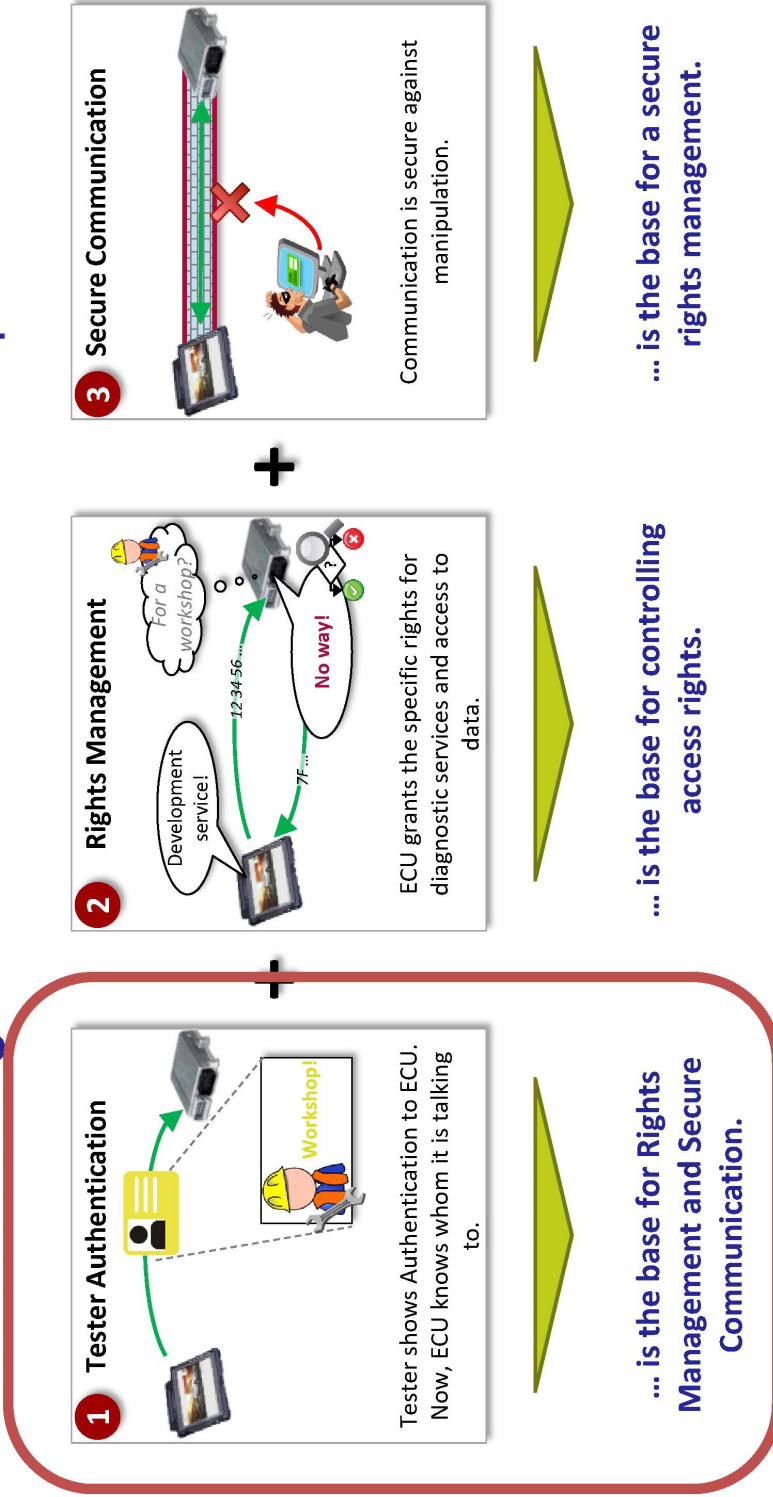
There is a big basis of common interests

- Authentication, Authorization and Secure Communication are adequate measures to address diagnostic security concerns
- Standardization is the right way to proceed
- Granularity of the security features is OEM dependent, but the mechanisms should be the same
- (At least a partial) Online approach is necessary
 - E.g. certificates with a limited lifetime

What to standardize in ISO WG2?



Secure Diagnosis has three main components:



Different Variants for Authentication have been discussed

Variant	Comment
1 RoutineControl (0x31) with standardized RID	<ul style="list-style-type: none"> + Quick & dirty - Quick & dirty + Keep diagnostic session handling „as it is“ - Special NRCs only for this RID + Keep existing SecurityAccess handling „as it is“ - Complex, would need to replace or massively enhance today's session handling - Proposed authentication sequence requires at least two Steps (RQ-RS-RQ-RS → Challenge from ECU, Response from Test Tool), DiagnosticSessionControl provides only one (RQ-RS) - Special NRCs only for this Session
2 Additional Diagnostic Session	
3 SecurityAccess (0x27)	<ul style="list-style-type: none"> + Proposed authentication sequence is very similar to existing SecurityAccess sequence - but: currently only one security level at a time (→ it would not be possible to combine authentication and further SecurityAccesses, e.g. airbag deployment as defined in ISO 26021) - but: additional parameters necessary (e.g. within response on sendKey request) + Keep existing diagnostic session handling „as it is“ - Special NRCs only for this security level
4 New SID „Authentication“	<ul style="list-style-type: none"> + Clean approach + usable for other certificate verification besides authentication? + Keep existing diagnostic session handling „as it is“ + Keep existing SecurityAccess handling „as it is“ - New SID, more specification work to be done?
5 Other?	?

SELECTED BY GROUP

Proposal for UDS service „Authentication“ has been created in five steps:

1. Initial proposal based on certificates has been created by Manuel Henle,
Daimler
2. Various comments from the group were collected, discussed and implemented
3. Approach without PKI and symmetric cryptography was proposed by Xin Ye,
Ford
4. Approach to extend the Ford proposal with asymmetric cryptography was
proposed by Andreas Sadler, Audi
5. In various working sessions, Manuel, Xin and Andreas merged the different
approaches into one proposal.
Many thanks for their great effort!



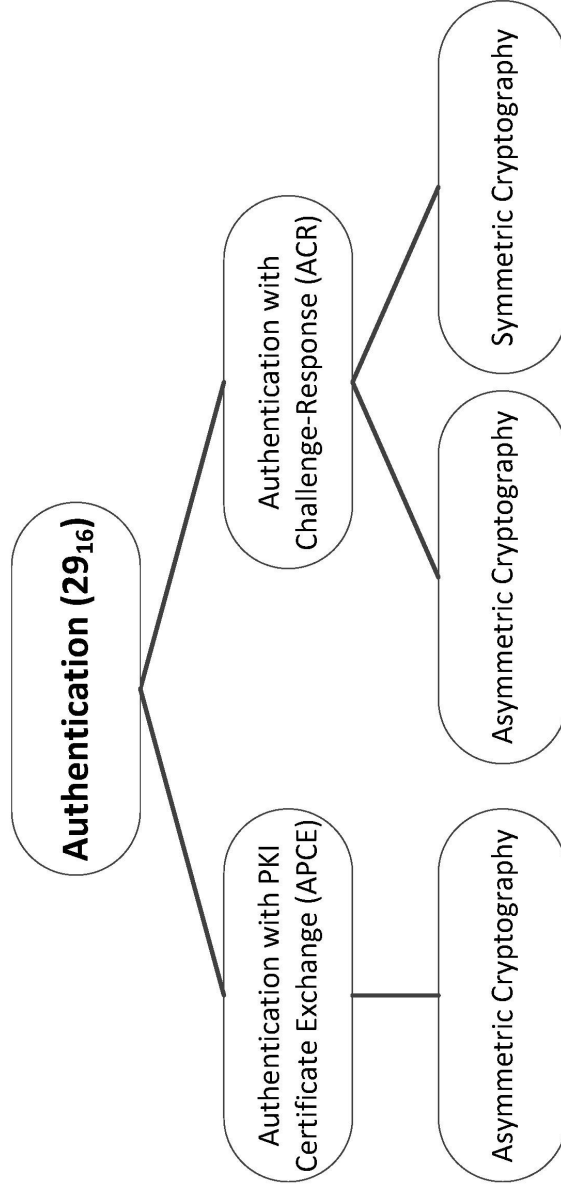
New SID Authentication (1/3) Document structure

- 3 Terms and definitions
- 10 Diagnostic and Communication Management functional unit
 - 10.6 Authentication (\$29) service
 - 10.6.1 Service Overview
 - 10.6.2 Authentication with PKI Certificate Exchange (APCE)
 - 10.6.3 Authentication with Challenge-Response (ACR)
 - 10.6.4 Common Requirements
 - 10.6.5 Request message
 - 10.6.6 Positive response message
 - 10.6.7 Supported negative response codes (NRC_)
 - 10.6.8 Message flow example(s) Authentication
 - Annex A (normative) Global parameter definitions
 - A.1 Negative response codes
 - Annex B (normative) Return functional unit data-parameter definitions
 - B.1 ReturnParameter definitions

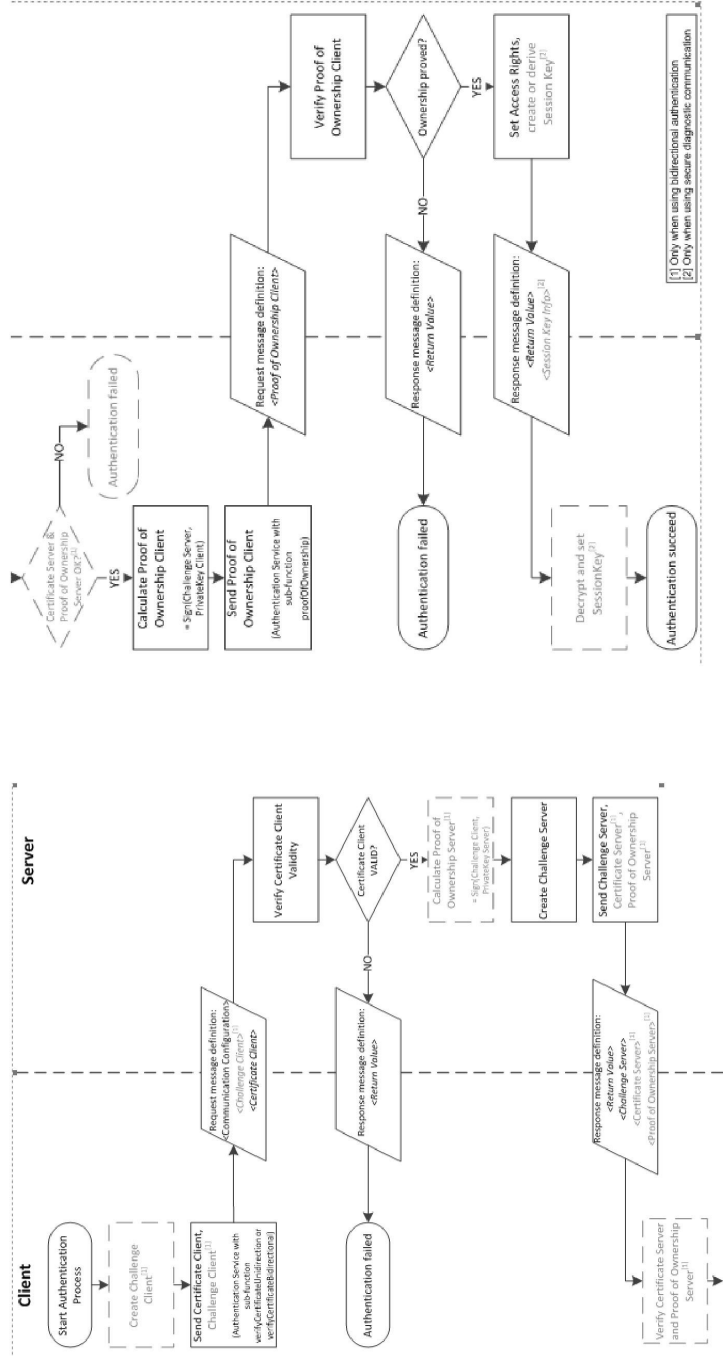
New: Chapter 10.6; Chapters with changes: 3, A.1, A.2



New SID Authentication (2/3) Overview



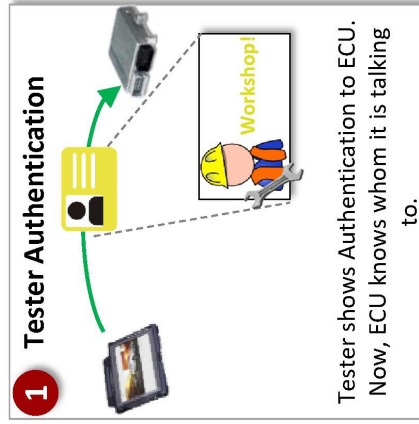
→ Will be shown using the Word draft document



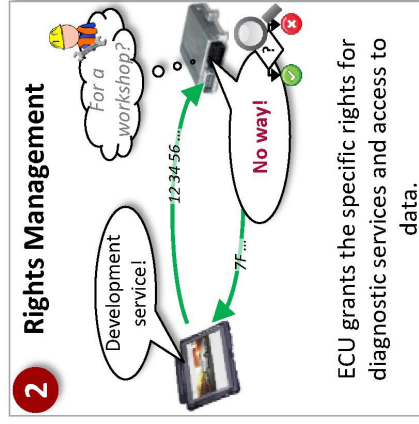
1. The new UDS service identifier has been assigned the working title \$29 „Authentication“ → Is number \$29 okay?
2. Assign the mnemonics according to the ISO rules
3. Subservices for symmetric and asymmetric cryptography are handled in one chapter instead of separate chapters. If this is not suitable, this can be changed based on a better proposal.
4. NRC for new Authentication (\$29) service :
 - Use NRC \$33 (“Security Access denied”) like for Security Access (\$27) OR
 - Introduce a new NRC e.g. \$34 (“Authentication denied”)?
5. **Implement the proposal in new ISO 14229-1 draft**

Next topic: Secure Communication

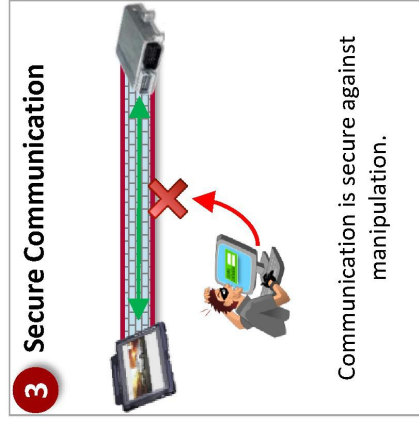
Secure Diagnosis has three main components:



... is the base for Rights
Management and Secure
Communication.



... is the base for controlling
access rights.



... is the base for a secure
rights management.

Variants for Secure Communication (1/2)

- Three Approaches have been shown and discussed
 - Using **UDS \$84** (Saul Scott, Tim Proctor, GM)
 - **Extend Autosar SecOC** (Manuel Henle, Daimler)
 - Using **DoIP and Internet mechanisms** (Andreas Sadler, Audi)
 - 4th approach – not discussed in project team:
 - Using UDS \$84 and Autosar SecOC (Mauro Cerrato, CNH Ind.)
- Every approach has different use cases, advantages and disadvantages.
- There was *no* recommendation out of the project team *for or against* one of the solutions

- In Autosar, work already started for the following topics:
 - Using UDS \$84
 - Information about already known changes to ISO14229-1 will be provided by Tim Proctor and Mauro Cerrato as a separate topic in the WG2 meeting
 - Extend Autosar SecOC
 - Currently, no changes in WG2 documents is necessary
- **Recommendation to WG2:**
Continue with already started developments in Autosar. After that come back to ISO with a proposal for standardization.
(Autosar timeline will be provided in the WG2 meeting)

- It was very helpful that security experts joined the WG2 project team.
- A camera-ready“ proposal for a UDS authentication service was jointly developed.
- Now, it is up to WG2 to make the next step and include the proposal in ISO 14229-1.
- For secure communication, no clear path was advised by the project team. It is recommended that the results from Autosar will be proposed for implementation in ISO.

Many thanks to all the project team participants for their constructive, disciplined and valuable work!

SVI Data Objects and Message Formats

CONFIDENTIAL

AAI-ACA-0022371

Data Dictionary – ISO 21184

The Secure Vehicle Interface (SVI) is a set of functional components that locally connect a vehicle ITS station (V-ITS-S) to a vehicle in a secure manner with minimum latency.

This International Standard contains specifications for a common description of vehicle-related information to be made available in a safe and secure manner to distributed ITS applications.

The output will be a dictionary of data objects and messages described using ASN.1 containing information available from vehicles that is relevant for C-ITS applications and services including time-critical safety applications and automated driving.

This International Standard will also contain specifications for the process of registering new data objects. The data registry process describes tasks and responsibilities of stakeholders in order to support the use cases specified by authorities and other stakeholders.

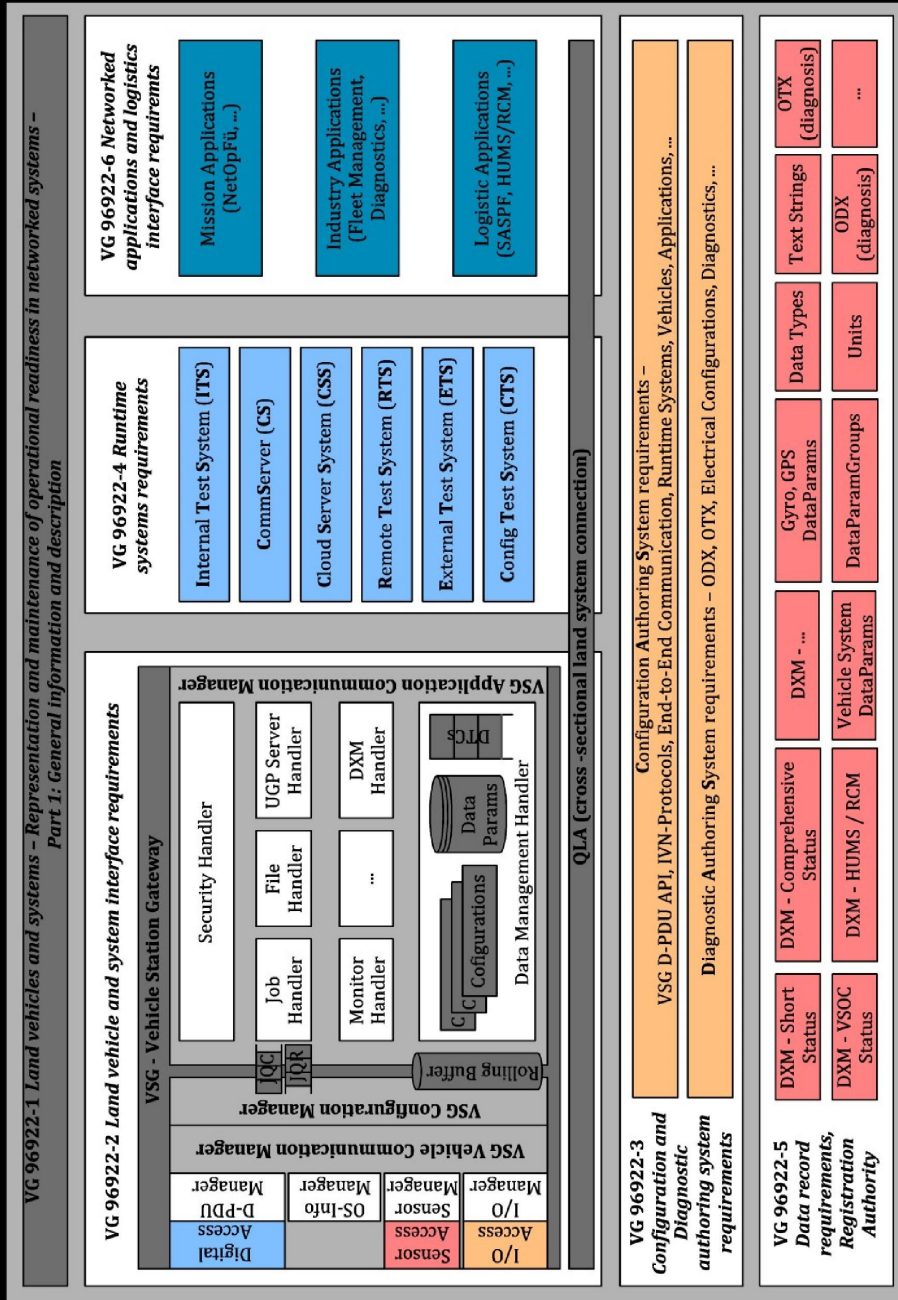
Example SVI Retrofit Implementation

Retrofitting Existing Road Vehicles with a SVI Compliant Solution

CONFIDENTIAL

AAI-ACA-0022373

Sample SVI Implementation



Project Descriptions – DIN VG 96922

VG 96922-1 General information and description

The frame document providing an overview about the purpose and content of all parts of VG 96922.

VG 96922-2 Land vehicle and system interface requirements

Defines the requirements of a multi-brand interface to access required data relevant for operational readiness. ISO references include: ISO 22900, 22901, 18314-2 & 13185-2

VG 96922 -3 Diagnostic and Configuration authoring system requirements

Requirements for the multi-brand configuration and diagnostic authoring system. ISO references include: ISO 22900, 22901, 13209, 13209, 13184-2 & 13185-2.

VG 96922-4 Runtime system requirements

Requirements of the multi-brand runtime system. ISO references include ISO 22900, 22901, 13209, 13185-2

VG 96922-5 Data record requirements, Registration Authority

Requirements of data structuring, data contents, data formats and information including their weighting with regarding representation and maintenance of operational readiness in networked systems. ISO references include: ISO 22901

VG 96922-6 Networked system applications, interface requirements

defines the interface requirements between the applications which provide the status information in the networked systems.

Referenced standards

Note: the following documents refer to SVI as the Vehicle Station Gateway (VSG)

ISO 7498-1, <i>Information processing systems; Open Systems Interconnection; basis reference model</i>	ISO 22901 (all parts), <i>Road vehicles — Open Diagnostic data eXchange (ODX)</i>	SAE J2186, <i>E/E Data Link Security</i>
ISO 13184-2, <i>Intelligent transport systems (ITS) — Guidance protocol via personal ITS station for Open Systems Interconnection — Basic Reference advisory safety systems — Part 2: Road guidance protocol (RGP) requirements and specification</i>	ISO /IEC 10731-1:1994, <i>Information technology — Open Systems Interconnection — Basic Reference Model — Conventions for the definition of OSI services</i>	VG 95287 (all parts), <i>Design of testable products</i>
ISO 13185-2, <i>Intelligent transport systems (ITS) — Vehicle interface for provisioning and support of ITS Implementation of WWH-OBD communication services — Part 2: Unified gateway protocol (UGP) requirements and specification for vehicle-ITS-station gateway (V-ITS-SG) interface</i>	ISO 27145 (all parts), <i>Road vehicles — Implementation of WWH-OBD communication requirements</i>	VG 95916 (all parts), <i>Electrical Systems for Land Vehicles</i>
ISO 13209 (all parts), <i>Road vehicles — Open Test sequence eXchange (OTX)</i>	DIN EN 61508, <i>Functional safety of electrical / electronic / programmable electronic safety-related systems</i>	SAE J2186, <i>E/E Data Link Security</i>
ISO 13400-4, <i>Road vehicles — Diagnostic SAE J1930-DA, Digital Annex of Electrical/communication over Internet Protocol (DoIP) — Part Electronic Systems Diagnostic Terms, Definitions, 4: Ethernet-based high-speed data link connector</i>	SAE J1930-DA, <i>Digital Annex of Electrical/communication over Internet Protocol (DoIP) — Part Electronic Systems Diagnostic Terms, Definitions, Abbreviations, and Acronyms</i>	VG 95287 (all parts), <i>Design of testable products</i>
ISO 14229 (all parts), <i>Road vehicles — Unified diagnostic services (UDS)</i>	SAE J1979-DA, <i>Digital Annex of E/E Diagnostic Test Modes</i>	VG 95916 (all parts), <i>Electrical Systems for Land Vehicles</i>
ISO 15031-3, <i>Road vehicles — Communication SAE J2012-DA, Digital Annex of Diagnostic Trouble between vehicle and external equipment for emissions- Code Definitions related diagnostics — Part 3: Diagnostic connector and related electrical circuits: Specification and use</i>	SAE J2012-DA, <i>Digital Annex of Diagnostic Trouble between vehicle and external equipment for emissions- Code Definitions</i>	

References Courtesy of Concepts & Services Consulting

CONFIDENTIAL

AAI-ACA-0022376

Benefits

- SVI can be implemented in both new and used vehicles
- The same standardized and secure interface supports remote and direct connected diagnostics, Intelligent Transport Systems V2I, V2V and V2X integration requirements
- Vehicle data elements mapped to a single SVI metadata label reduces the need for proprietary documentation
- Vehicle manufacturers retain full control over how SVI is implemented in new car construction and how the information delivered over vehicle networks is mapped to metadata definitions

Next Steps

- Review existing Secure Vehicle Interface documentation (SVI, VSG, VIM, etc.) published by ISO, SAE and DIN
- Encourage stakeholders representing vehicle manufacturers and their suppliers to participate with the automotive aftermarket in the SAE project defining an ITS compliant Vehicle Interface Methodology (VIM) securing wireless and OBDII port communications
- Collaborate with aftermarket engineers in developing a single set of cybersecurity policies and implementation guidelines applicable to retrofit and new vehicle VIM implementations
- Publish the completed projects as SAE/ISO standards based on the existing ISO TC22/SC31 standards agreement for joint publication

Exhibit 503



December 13, 2016

Jack Pokrzywa, Manager, Ground Vehicle Standards
Tim Weisenberger, Ground Vehicle Project Specialist
SAE International
400 Commonwealth Drive
Warrendale, PA 15096

Dear Mr. Pokrzywa and Mr. Weisenberger:

Recognizing SAE International's leadership in developing automotive engineering standards that have underpinned the advancement of vehicle technology in North America over the past 100 years, we are writing to you today to encourage the organization's prompt engagement on matters relating to the security of vehicle data and vehicle systems, specifically the *Secure Vehicle Interface (SVI)*.

Earlier this month, 36 representatives from 9 automobile manufacturers and 9 automotive and aftermarket trade groups met in Las Vegas to hear details of a presentation on the SVI. On its surface, the SVI may present a solution that addresses a number of concerns previously identified. While many qualified that further study was certainly needed, there was, at the very least, unanimity amongst those in attendance that a further vetting of the SVI concept was warranted.

While representing different segments of the automotive industry, each signatory understands how vital cybersecurity is to both public safety and public acceptance of new vehicle technologies. Likewise, we understand the need for the independent repair community to continue to have access to vehicle repair and service information. This ensures the swift and accurate repair of vehicles – both new and old.

Appreciating the gravity of this subject, the undersigned have met numerous times over many months to discuss the various opportunities and challenges presented by expanded access to vehicle data, and the necessity to deliver such data securely in order to enhance and improve customer experience throughout the vehicle ownership lifecycle. In these discussions to find viable solutions, we have recognized the many potential downfalls that could result from non-secure vehicle systems. Over the course of these meetings, it has become clear that any solution will require a thorough understanding of complex vehicle systems, cybersecurity, diagnostic tools, and vehicle service generally. Moreover, to have a viable solution, engineers will need to systematically define the problem and then develop solutions to address identified shortcomings. Such expert knowledge and processes are the very hallmarks of SAE, making your organization best situated to undertake this endeavor.

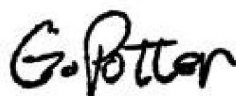
It is in light of that agreement that we write to you today. The undersigned believe that it is appropriate for SAE International to convene a working group(s) of industry engineers to properly investigate the merits of the SVI or other methods, and ascertain whether they could provide the solution on this matter that is greatly needed. For example, SAE convened a workgroup including automakers, aftermarket, government agencies (National Highway Traffic Safety Administration, National Institute of Standards and Technology, and California Air Resources Board) on 1-Dec-2016 to discuss methods to secure the on-board diagnostic connector. Representatives of the many companies our organizations represent are committed to working through this significant challenge with SAE's coordination and oversight.

Thank you in advance for your consideration of this request. We offer our support in any way deemed useful to further this examination.

Respectfully offered,



William J. Hanvey
Auto Care Association
President and CEO



Greg Potter
Engine and Tool Institute
Executive Manage



Dan Risley
Automotive Service Association
President and Executive Director



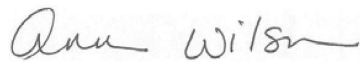
Ray Pohlman
Coalition for Auto Repair Equality
President



Bill Long
Automotive Aftermarket Suppliers
Association
President and COO



Jean-François Champagne
Automotive Industries Association
of Canada
President



Ann Wilson
Motor and Equipment Manufacturers Association
Senior Vice President



John Nielsen
AAA National Office
Managing Director, Engineering and Repair



Ellen J. Gleberman
Association of Global Automakers, Inc.
Executive Vice President & General Counsel



Amy Brink
Alliance of Automobile Manufacturers
Vice-President of State Affairs

Exhibit 4



September 18, 2017

To:

Mr. William J. Hanvey, President and CEO, Auto Care Association
Mr. Greg Potter, Executive Manager, Engine and Tool Institute
Mr. Dan Risley, President and Executive Director, Automotive Service Association
Mr. Ray Pohlman, President, Coalition for Auto Repair Equality
Mr. Bill Long, President and COO, Automotive Aftermarket Suppliers Association
Mr. Jean-Francois Champagne, President, Automotive Industries Association of Canada
Ms. Ann Wilson, Senior Vice President, Motor and Equipment Manufacturers Association
Mr. John Nielsen, Managing Director, Engineering and Repair, AAA National Office
Ms. Ellen J. Gleberman, Executive Vice President & General Counsel, Association of Global Automakers, Inc.
Ms. Amy Brink, Vice-President of State Affairs, Alliance of Automobile Manufacturers

Subject: Your letter dated December 13, 2016

Dear Mr. Hanvey, Mr. Potter, Mr. Risley, Mr. Pohlman, Mr. Long, Mr. Champagne, Ms. Wilson, Mr. Nielsen, Ms. Gleberman, and Ms. Brink:

This letter is in response to your letter dated December 13, 2016 regarding security of vehicle data and vehicle systems, specifically the Secure Vehicle Interface. First, we want to address the issues which helped SAE gather the industry to address vehicle interface security, then update you on the progress SAE has made in addressing this acute topic, and finally discuss our planned activities moving forward.

On September 12, 2016, The House of Representatives Committee on Energy and Commerce sent a letter to NHTSA to highlight their concern about OBD II security with their specific "request that NHTSA convene an industry-wide effort to develop a plan of action for addressing the risk posed by the existence of the OBD-II port in the modern vehicle ecosystem." Shortly thereafter, on September 28, NHTSA requested SAE to take the lead and convene an industry group to examine the issue. NHTSA followed with response to the House Committee on October 14 to highlight SAE's role in addressing their concern.

SAE responded to NHTSA's request by hosting two workshops on December 1, 2016 and on January 30, 2017 to discuss the issue of OBDII security and identify an appropriate work item to address it. In attendance were auto manufacturers of light vehicles and heavy trucks and buses, suppliers, cyber security experts, experts from government, including regulators, and associations including signatories to your December 13 letter.

The discussions were open and comprehensive including security concerns beyond the narrow focus of the OBD II port and specific discussion of Secure Vehicle Interface and

other approaches. The first work item was tightly scoped to address concern of the House Committee on OBD II port security, with the goal to complete by the end of 2017.

A new Committee called the Data Link Connector Vehicle Security was created to focus on the first work item but also to allow broader discussion of vehicle interface security. The first committee meeting was on February 17, 2017. The group began work in earnest on J3138 "Guidance for securing the Data Link Connector (DLC)" which provides best practices for securing the OBD-II port and addresses the House Committee request to NHTSA to secure the OBDII port as a diagnostics and regulatory vehicle interface. They continue to meet monthly via Webex and teleconference.

By March, a new SAE Information Report called J3146 "Survey of practices for securing the interface through the Data Link Connector (DLC)" was initiated to codify information about standards and research efforts to address the broader security of vehicle interface. The goal of the report is to inform experts of the need to develop new standard work item(s) to address any broader vehicle interface security concerns members have including secure access to the vehicle in a trusted manner. This includes examination of Secure Vehicle Interface.

SAE has been very supportive of this information report and SAE experts' desire to examine vehicle security. Development of any further work items hinges on the input and support of all segments of the automotive industry- original equipment manufacturers, suppliers, aftermarket companies as well as trade associations. The issue of the Secure Vehicle Interface has been discussed in various working groups around the world with no measurable outcome to date and it remains to be open.

A separate effort to create a Secured Vehicle Interface for purposes other than diagnostics and regulatory requirements has been discussed within SAE but we are not aware of any requirements or regulation for vehicle manufacturers to provide this additional vehicle interface (separately or integrated with the diagnostic port). If such a requirement were needed, we expect many of the best practices from the Data Link Connector Vehicle Security Committee and the J3138 standard to apply.

However, these requirements may not be sufficient to cover use cases beyond the current and expected future OBD-II diagnostics and regulatory requirements or they may be in conflict when used to access the OBD-II port for purposes beyond its diagnostic and regulatory intent.

Please contact me directly if you require more information.

Sincerely,

A handwritten signature in black ink, appearing to read "Jack Pokrzywa".

Jack Pokrzywa, Director, Global Ground Vehicle Standards, SAE International

cc: SAE Motor Vehicle Council

Exhibit 505

Message

From: Tim Turvey [/O=GM/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=B0A16E2173E14A7EAE8AACABF09C5B59-RZ5NV9]
Sent: 2/11/2019 9:22:26 PM
To: Aaron Lowe [aaron.lowe@autocare.org]
CC: Bill Hanvey [bill.hanvey@autocare.org]; Pohlman, Ray [ray.pohlman@autozone.com]; McKinney, David [david.mckinney@autozone.com]; Finestone, Mark [mark.finstone@autozone.com]; Rhodes, Bill [bill.rhodes@autozone.com]; Joe Register [Joe.Register@autocare.org]; Paul Copses [paul.copses@gm.com]
Subject: Vehicle Data Access

Aaron,

I appreciate your prompt follow up to our recent discussion on the Right to Repair. As indicated in my January 24th response to Bill Rhodes, we are in the process of developing our position on the areas of safety, cybersecurity, and consumer privacy. We continue to keep the GM Senior Leadership Team that you met fully engaged. We have had discussions following our meeting and remain committed to getting back with you as soon as possible.

Best Regards,
 Tim

From: Aaron Lowe [mailto:aaron.lowe@autocare.org]
Sent: Friday, February 8, 2019 7:55 AM
To: Tim Turvey <tim.turvey@gm.com>
Cc: Bill Hanvey <bill.hanvey@autocare.org>; Pohlman, Ray <ray.pohlman@autozone.com>; McKinney, David <david.mckinney@autozone.com>; Finestone, Mark <mark.finstone@autozone.com>; Rhodes, Bill <bill.rhodes@autozone.com>; Joe Register <Joe.Register@autocare.org>
Subject: [EXTERNAL] Vehicle Data Access

Tim,

It was great meeting you a few weeks back and I think the discussion regarding the telematics issue was very helpful. Based on that discussion, I would like to set up a follow-up technical meeting to further discuss the Secure Vehicle Interface and how it could help ensure your GM vehicles are cyber secure, but still be able to allow access to critical repair data for consumers and the independent auto care industry. We would plan to have our technical team that worked to develop SVI attend in order to ensure that we can have an in depth discussion of this important issue.

I am sure everyone has a busy schedule, but I was thinking that we could look at a meeting in early March, either in Washington or Detroit, whichever is more convenient for your team. Let me know what dates might work for GM and we can hopefully find an acceptable date and time.

Thanks.

AARON LOWE
 Senior Vice President, Regulatory & Government Affairs
Liaison, Upholstery and Trim International Council(UTIC)

Auto Care Association
 7101 Wisconsin Ave., Suite 1300
 Bethesda, MD 20814
 Desk: 240-333-1021
 aaron.lowe@autocare.org

www.autocare.org

New Auto Care events are now open for registration! If you're a woman in auto care, under-40, or a cataloging professional, learn more and r

This email message is privileged and confidential. If you are not the intended recipient, please delete this message and notify the sender. Any views or opinions

Defendant's Exhibit G

Message

From: Bill Hanvey, MAAP [bill.hanvey@autocare.org]
Sent: 3/26/2019 12:02:39 PM
To: Rhodes, Bill [bill.rhodes@autozone.com]; Tim Turvey [tim.turvey@gm.com]
CC: Finestone, Mark [mark.finstone@autozone.com]; Pohlman, Ray [ray.pohlman@autozone.com]; Paul Copses [paul.copses@gm.com]
Subject: [EXTERNAL] RE: Telematics Data

Good Morning Tim,

I would like to echo Bill's comments regarding our commitment to keep the lines of communication open and would be more than willing to host a technical discussion on the secure vehicle interface here in Bethesda and continue our discussion on the Right to Repair MOU. Knowing that travel schedules are quite busy this time of year, perhaps you can recommend a few dates in May/June that would work for your team?

Bill

BILL HANVEY, MAAP
 President & CEO

Auto Care Association
 7101 Wisconsin Ave., Suite 1300
 Bethesda, MD 20814
 Desk: 240-333-1077
 bill.hanvey@autocare.org
 www.autocare.org



Get key stats on the state of the industry and what your association is doing for you. Read the new State of the Auto Care 2019 report: [autocare.org](#)

This email message is privileged and confidential. If you are not the intended recipient, please delete this message and notify the sender. Any views or opinions

From: Rhodes, Bill <bill.rhodes@autozone.com>
Sent: Monday, March 25, 2019 4:48 PM
To: Tim Turvey <tim.turvey@gm.com>
Cc: Finestone, Mark <mark.finstone@autozone.com>; Pohlman, Ray <ray.pohlman@autozone.com>; Bill Hanvey, MAAP <bill.hanvey@autocare.org>; Paul Copses <paul.copses@gm.com>
Subject: RE: Telematics Data

Tim,

Sorry for the delay, I had a couple of Board meetings last week.

We really appreciate your engagement and efforts to keep this moving forward. We are very interested in direct engagement to find those areas where we agree and can work together for the overall industry and especially our collective end consumers. We did put two issues on the table that while but related should probably be worked separately. While you all are formulating your response on the Vehicle Data topic, it does seem that our teams should work together to resolve our different points of view on GM's compliance with the current MOU regarding Right to Repair.

Should our smaller technical groups get together soon on the MOU? Bill Hanvey/Ray Pohlman could coordinate our participants.

I do hope that we can all develop ongoing direct dialogs as we all are serving the same customers.

Thanks for following up and I hope you are doing well,

Bill

From: Tim Turvey [mailto:tim.turvey@gm.com]

Sent: Thursday, March 14, 2019 1:47 PM

To: Rhodes, Bill <bill.rhodes@autozone.com>

Cc: Finestone, Mark <mark.finstone@autozone.com>; Pohlman, Ray <ray.pohlman@autozone.com>; Bill Hanvey <bill.hanvey@autocare.org>; Paul Copses <paul.copses@gm.com>

Subject: Telematics Data

Bill,

I wanted to let you know that we continue to work through the subject of data sharing within the GM Leadership team as discussed at our January 23rd meeting. I am comfortable this is receiving the proper attention at the highest levels within our company. Due to the complexity and breadth of this subject it is taking time to properly vet within GM. We look forward to getting back with you as soon as practical but did not want to let more time go by without touching base.

If you have any questions, please let me know. Thank you for your continued partnership.

Sincerely,

Tim Turvey

**GM Global Vice President
Customer Care & Aftersales**

Nothing in this message is intended to constitute an electronic signature unless a specific statement to the contrary is included in this message.

Confidentiality Note: This message is intended only for the person or entity to which it is addressed. It may contain confidential and/or privileged material. Any review, transmission, dissemination or other use, or taking of any action in reliance upon this message by persons or entities other than the intended recipient is prohibited and may be unlawful. If you received this message in error, please contact the sender and delete it from your computer.

Defendant's Exhibit E



Independence drives us.

www.autocare.org



Secure ITS Framework & SVI

Global Automakers Offices

February 12, 2019

Secure Intelligent Transportation System Framework (SIF)

Despite the fact that most Intelligent Transportation System services (ITS/C-ITS) have been standardized for over a decade, an essential aspect of these communication frameworks had eluded experts:

“How can we resolve the need for absolute trust in the reliability and security of data, versus the need to share this data between services, while adhering to the emerging privacy requirements such as those expressed in GDPR?”

The solution to this problem was defined in ISO TC204 and the ramifications for vehicle communications are significant!



ISO ITS Security Specifications



ISO TS 21177 Intelligent transport systems -- ITS station security services for secure session establishment and authentication between trusted devices



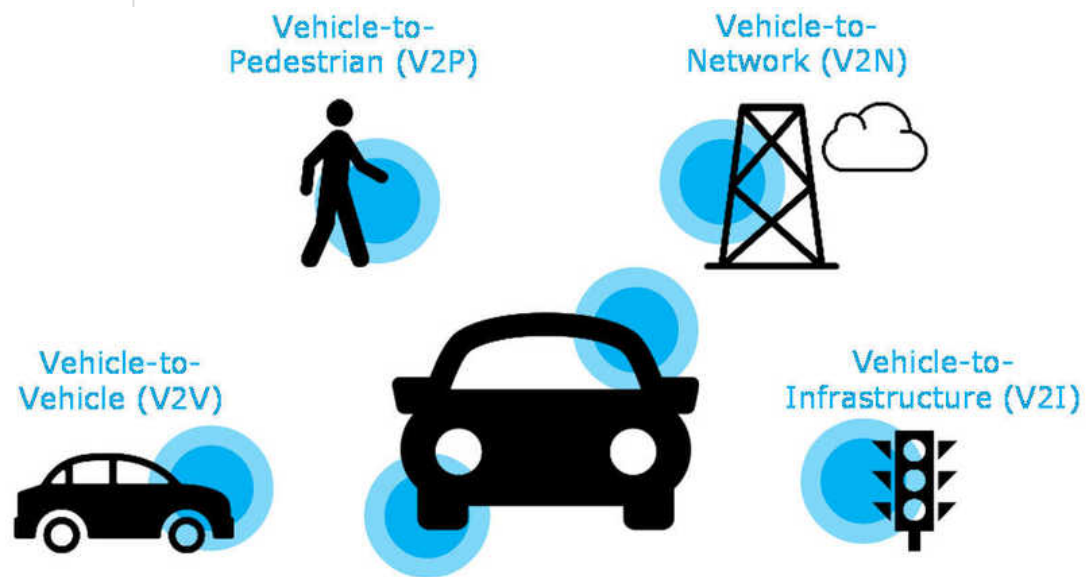
ISO TS 21185 Intelligent transport systems -- Communication profiles for secure connections between trusted devices



ISO TS 21184 Intelligent transport systems -- Management of messages containing information of sensor and control networks specified in data dictionaries

SVI Uses SIF to Secure Vehicle Communications

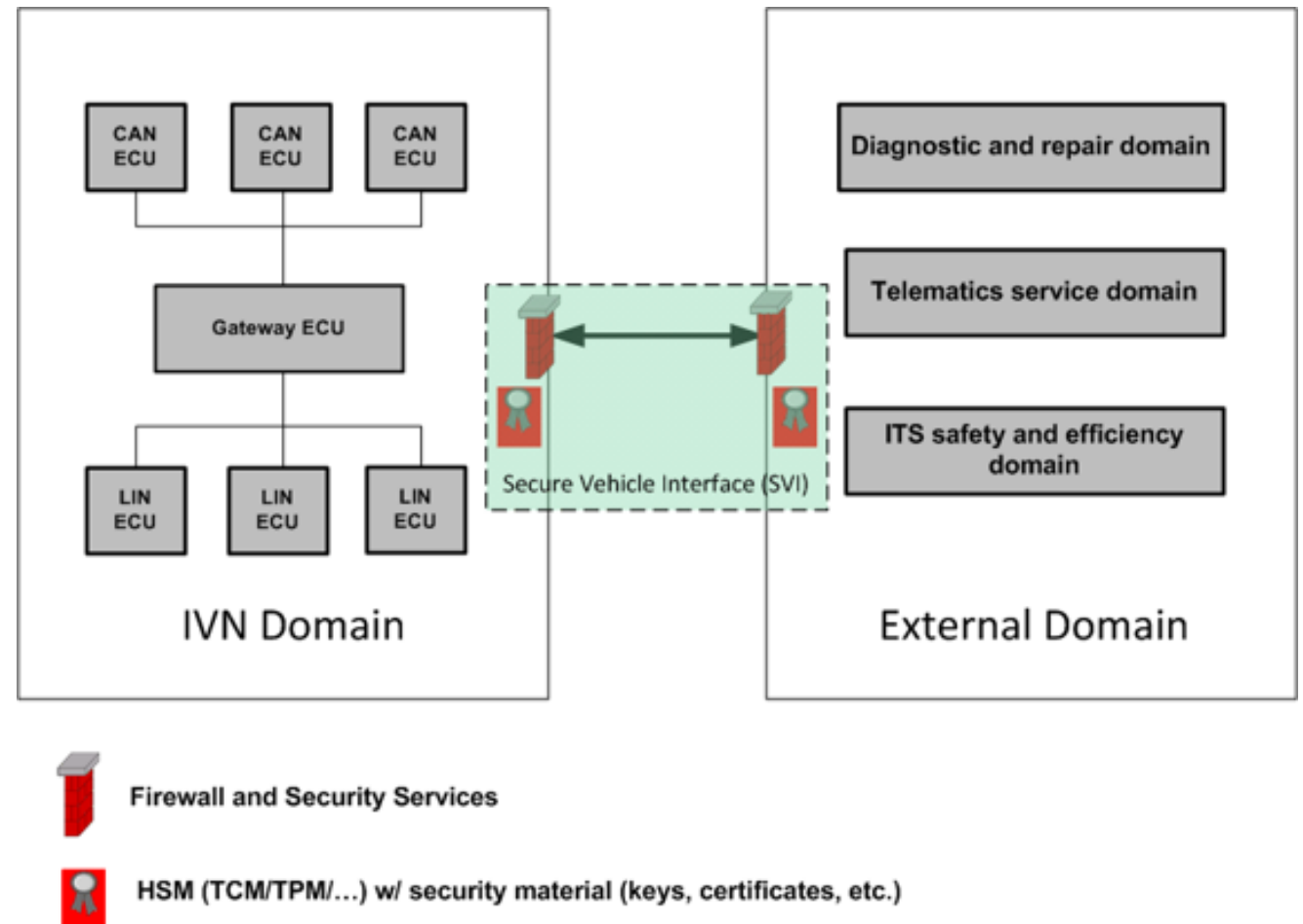
The Secure Vehicle Interface (SVI) is a bidirectional design based on the ITS station & SIF security standards, which enables secure, standardized and direct access to in-vehicle networks



Implementations of SVI are Applicable in both ITS
& IoT Vehicle Communication Solutions

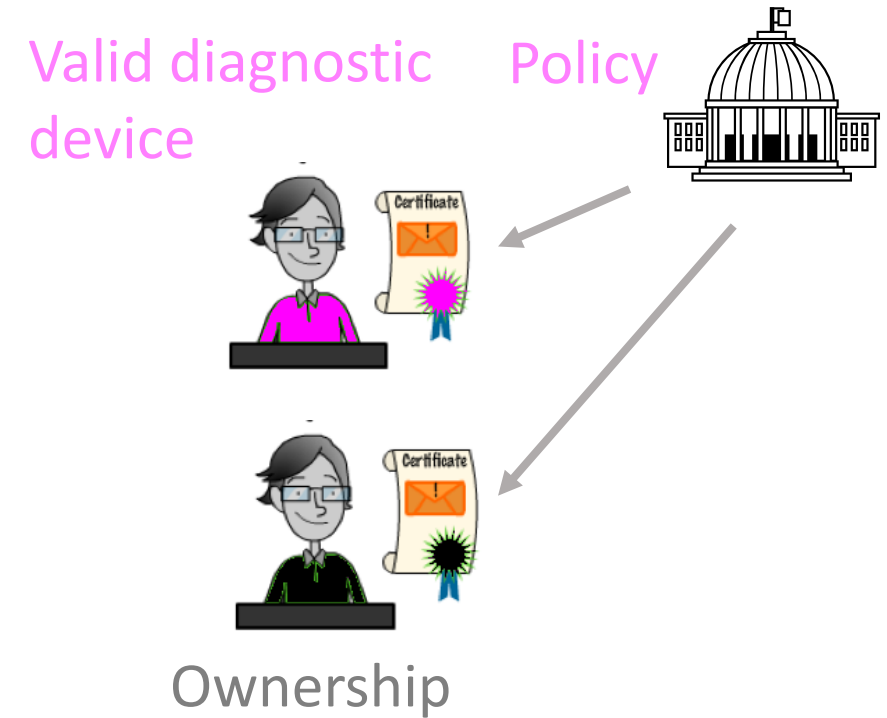
SVI = Secure In-Vehicle Trusted ITS Station

- SVI defines the interface between internal vehicle networks (IVN) and external devices, networks, and applications, enabling secure information exchange between the two.
- Two firewalled interfaces with Hardware Security Modules protect both wired or wireless connections.
- Identity and access to the IVN is managed using standardized internet security techniques (PKI infrastructure & digital certificates).

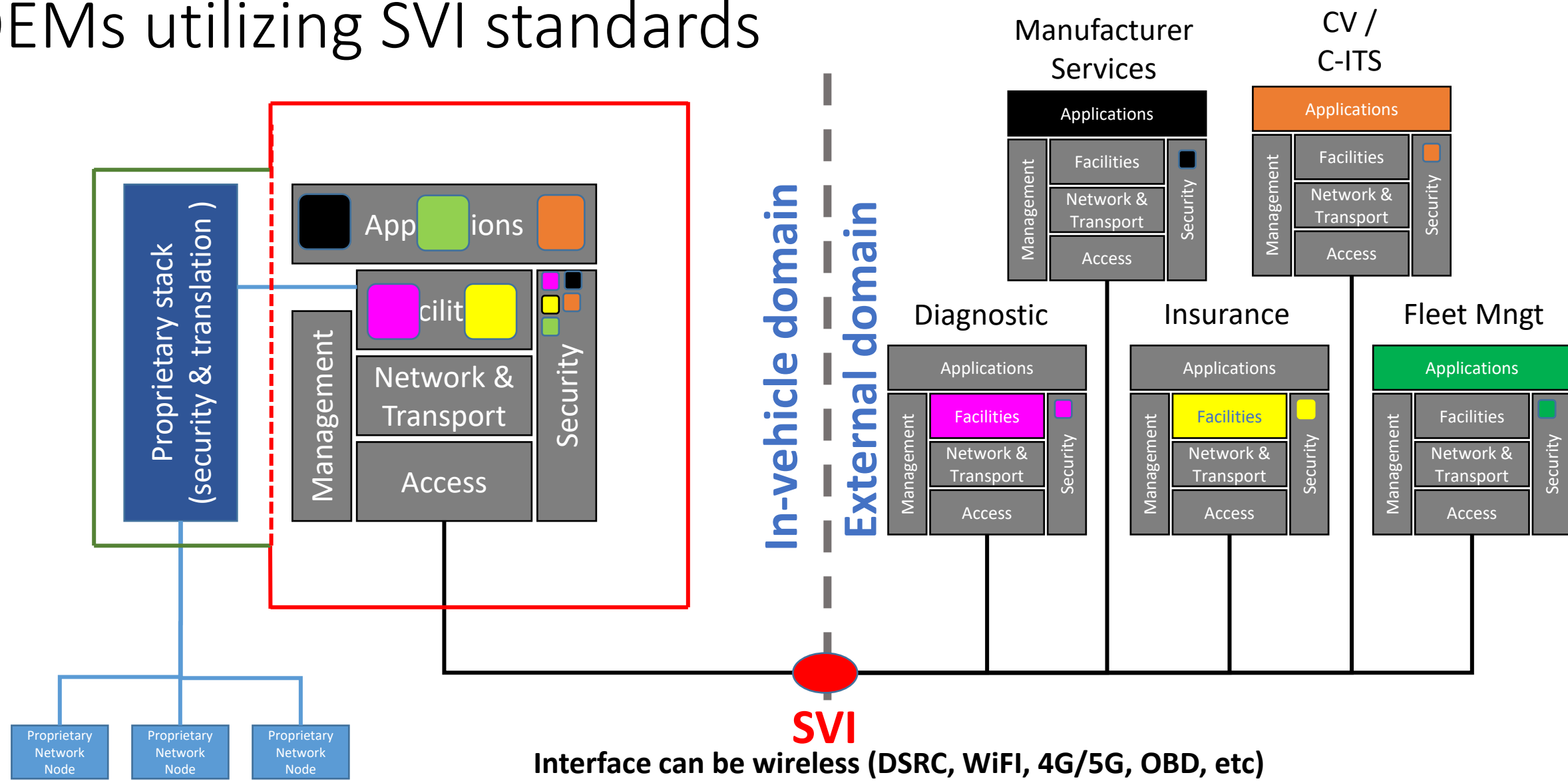


Security: Authentication / Authorization

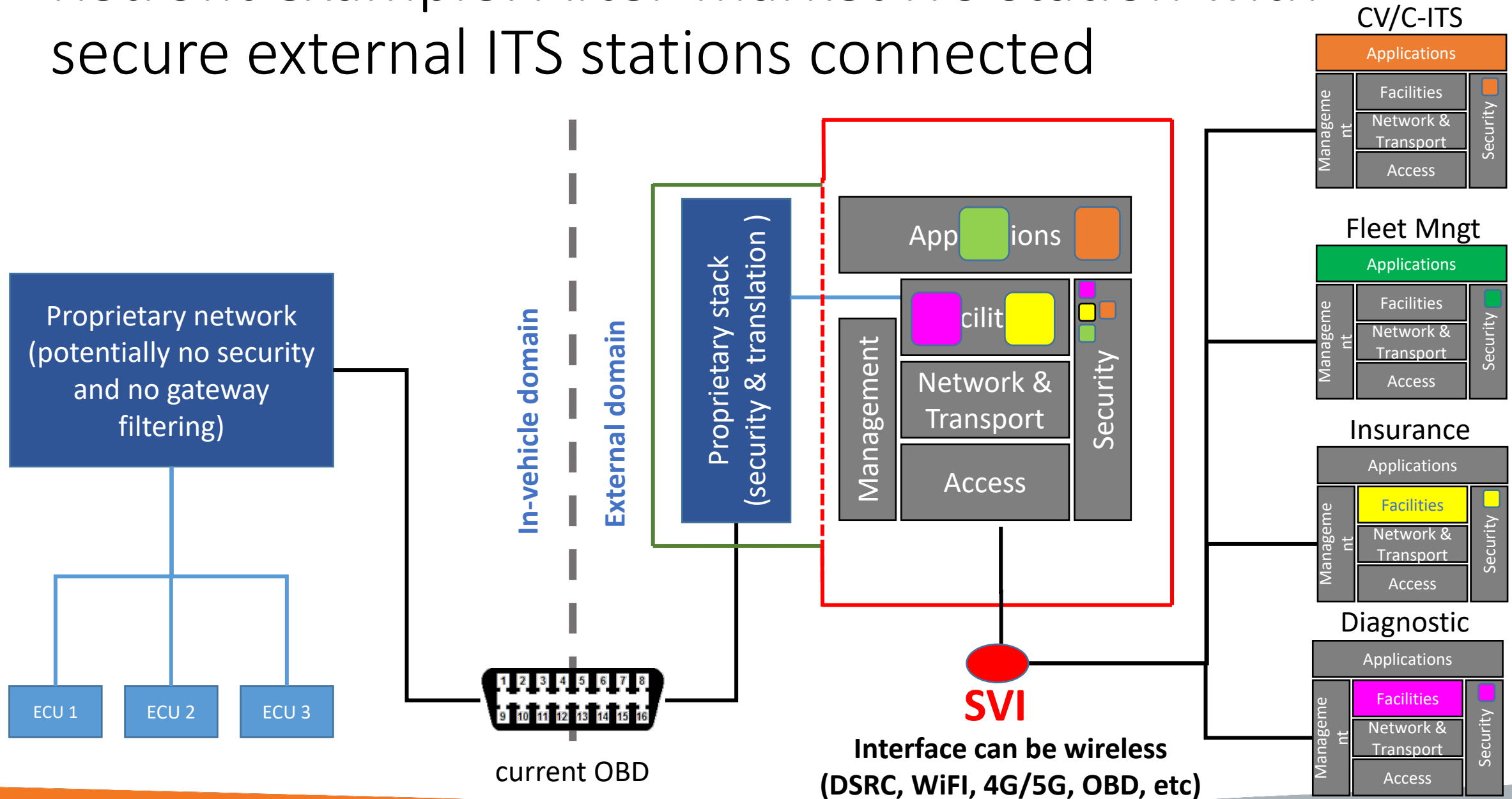
- Policy authorities and certificate authorities are already being established to support C-ITS
- This organizational structure can also support authentication and authorization for SVI
- OEMs can enforce reasonable security policies on certificate issuance and freshness
 - OEM security concerns are real and must be taken into account
- However, in this model OEMs are not real-time gatekeepers of access to the information
 - Nevertheless, their security requirements are met



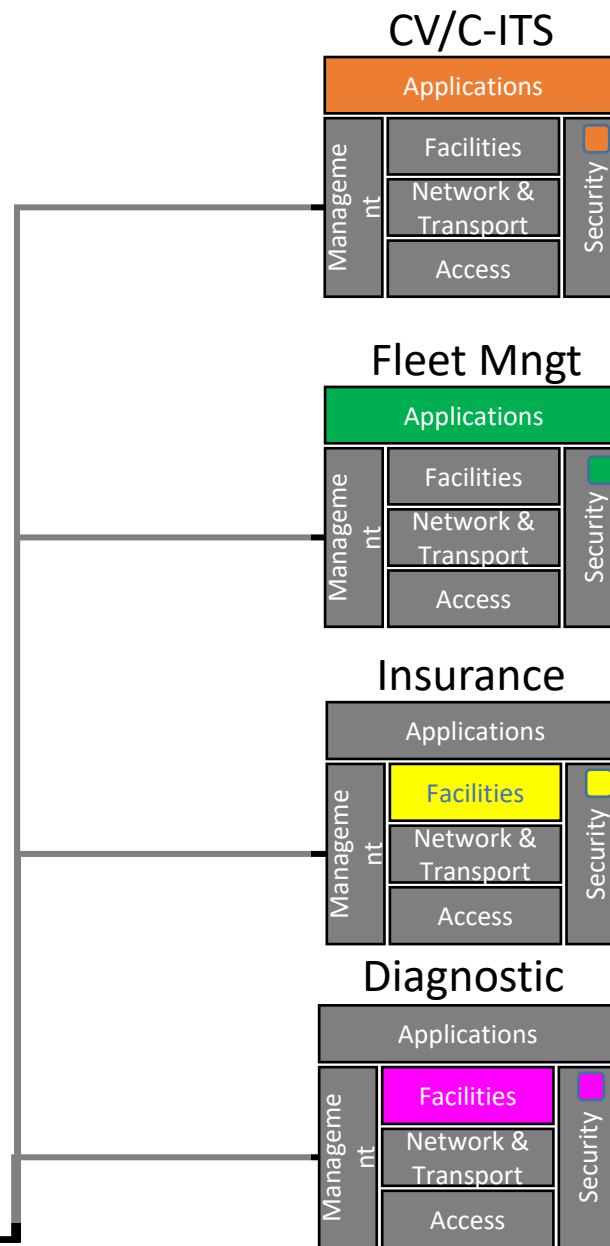
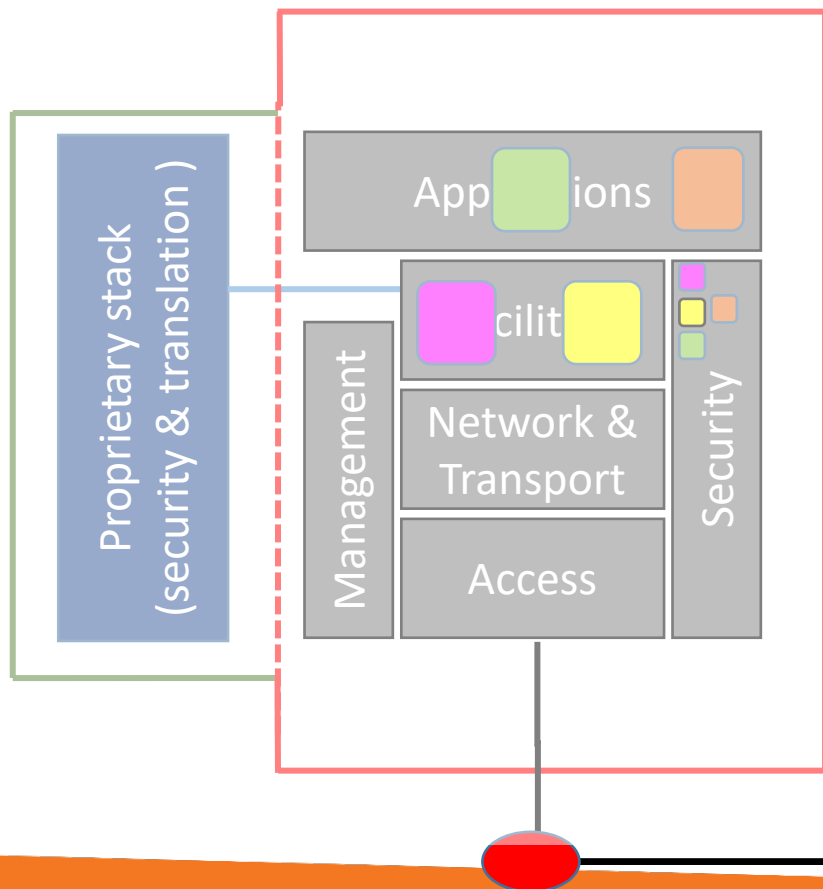
Example: Multiple after-market services with OEMs utilizing SVI standards



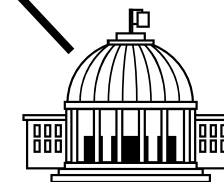
Retrofit example: After-market ITS station with secure external ITS stations connected



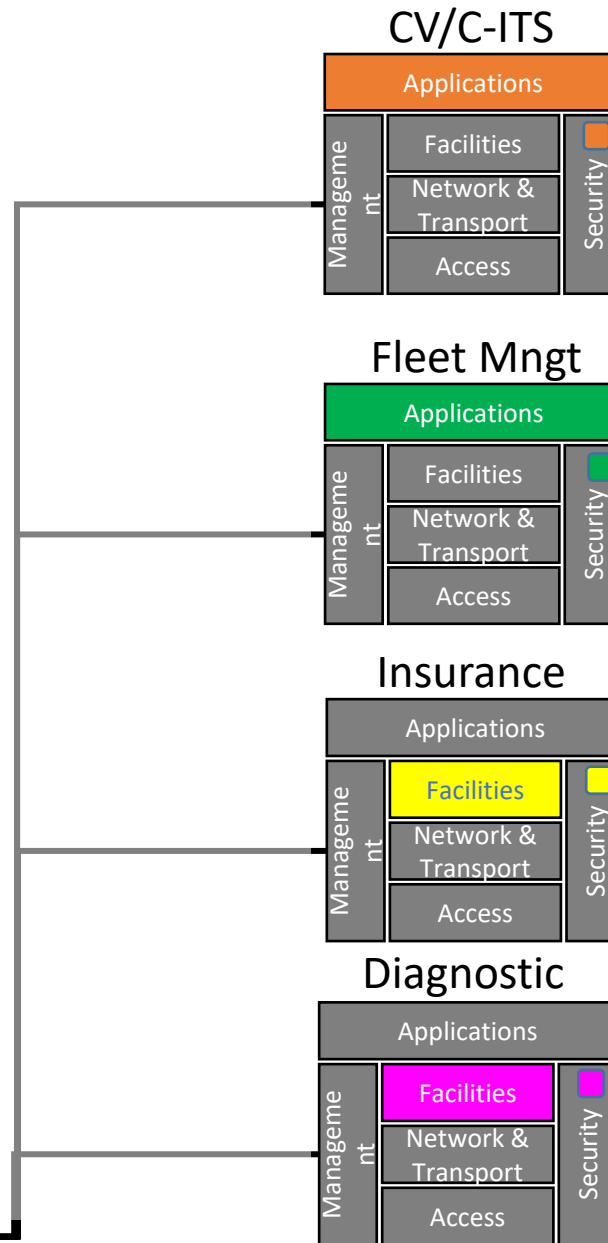
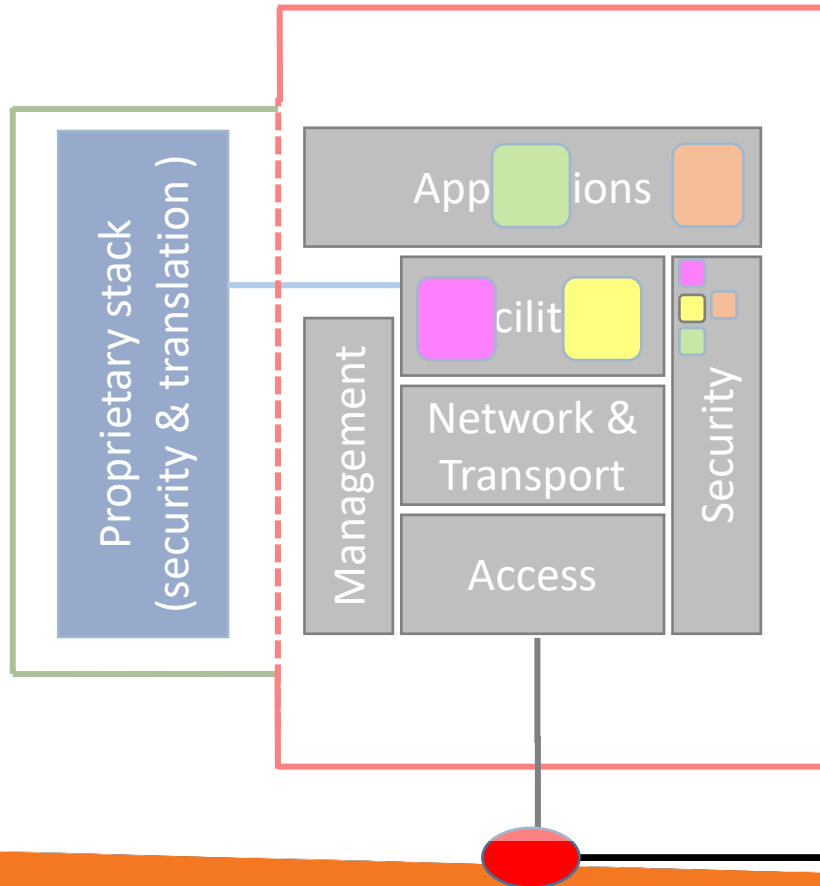
Security: Authentication / Authorization



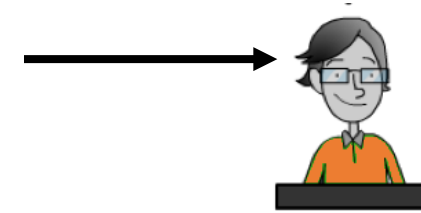
Policy



Security: Authentication / Authorization



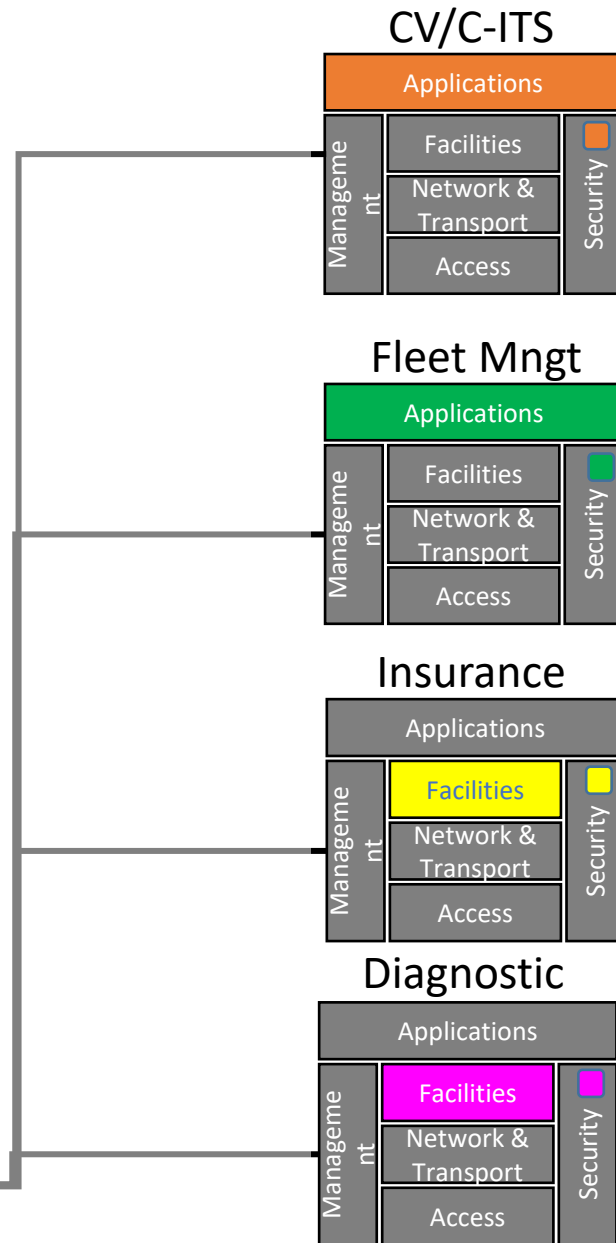
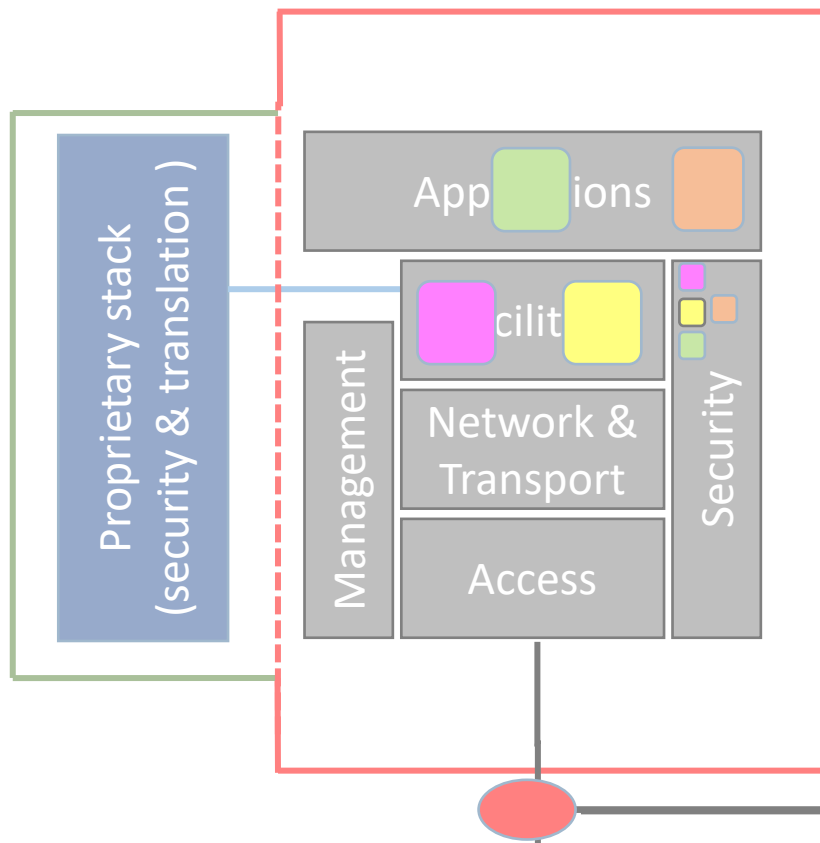
Proof: valid C-ITS Application



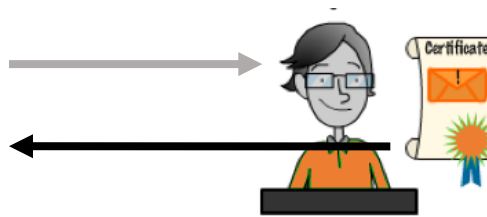
Policy



Security: Authentication / Authorization

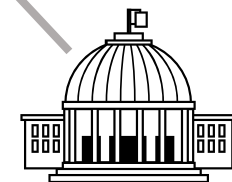


Proof: valid C-ITS Application

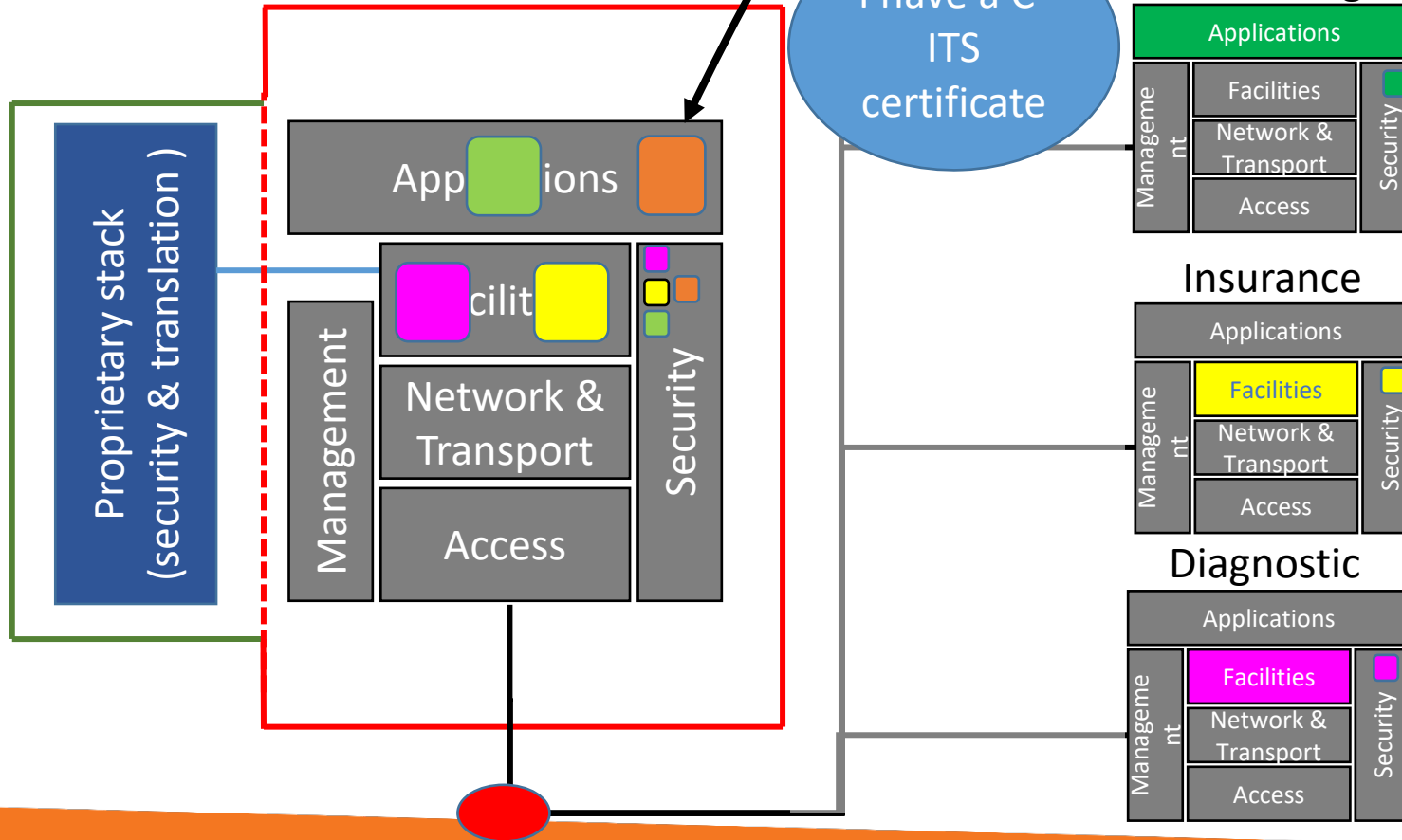


Certificate

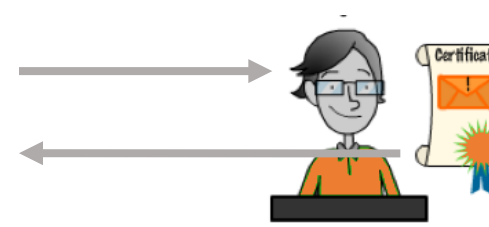
Policy



Security: Authentication / Authorization



Proof: valid C-ITS Application

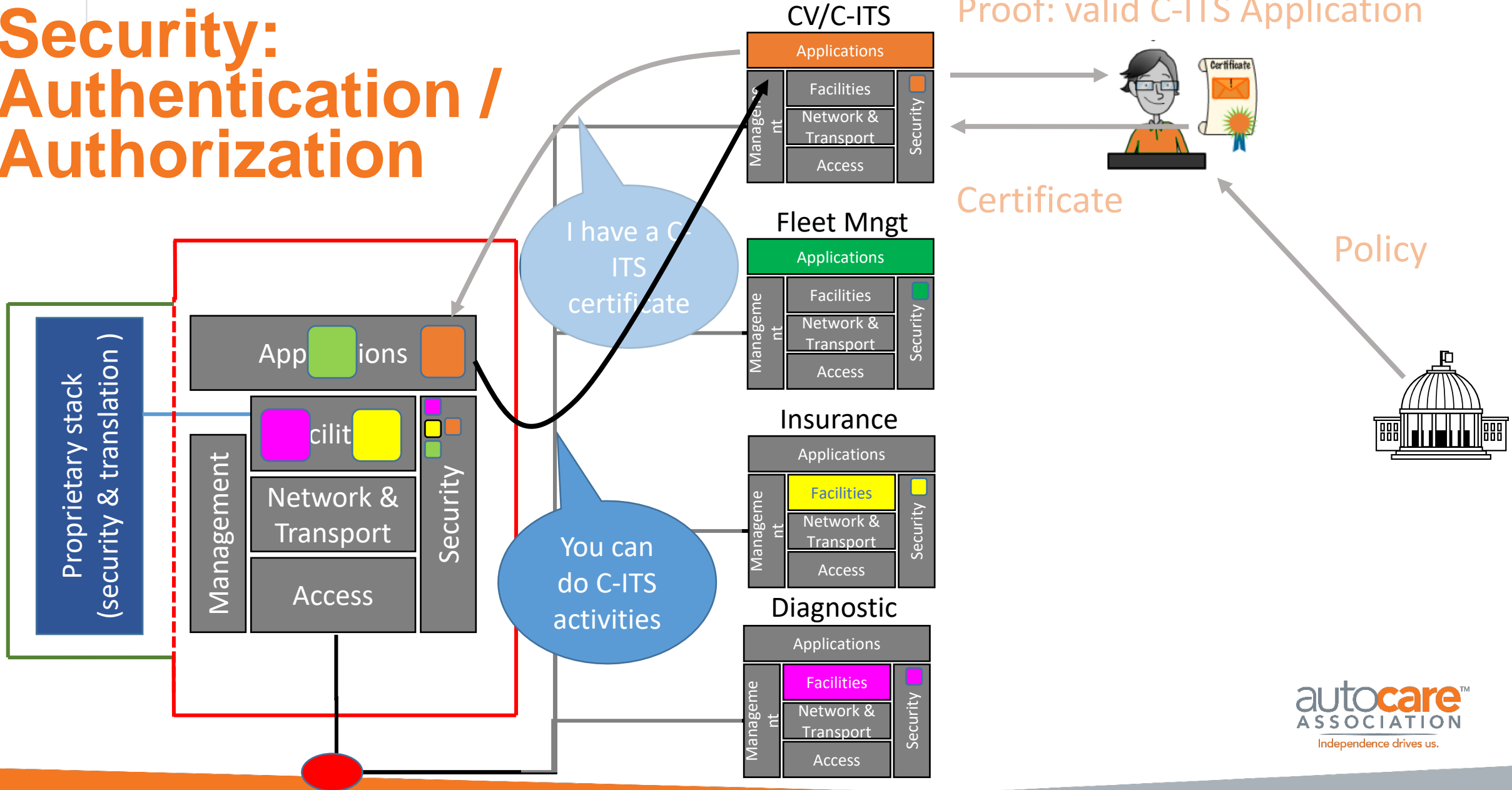


Certificate

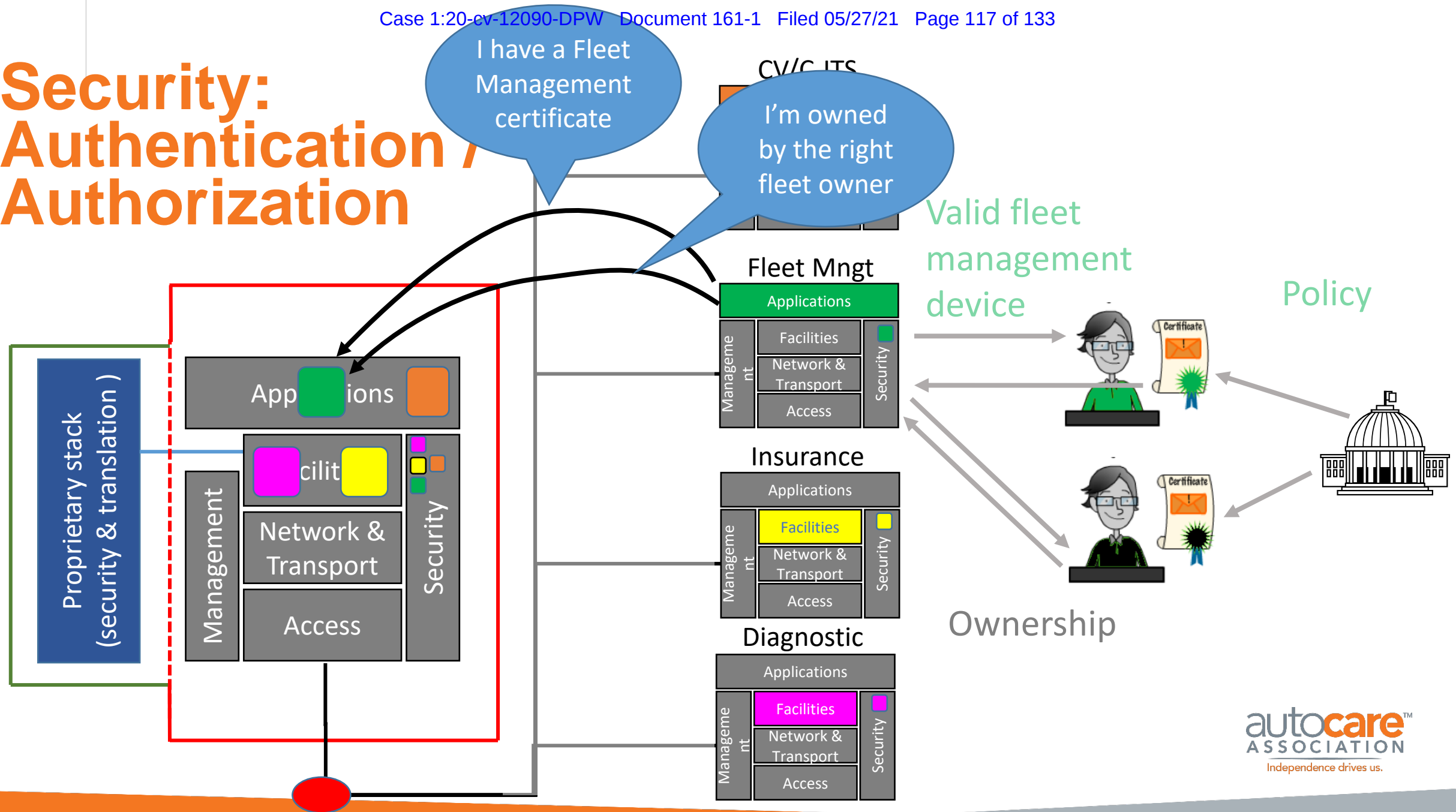
Policy



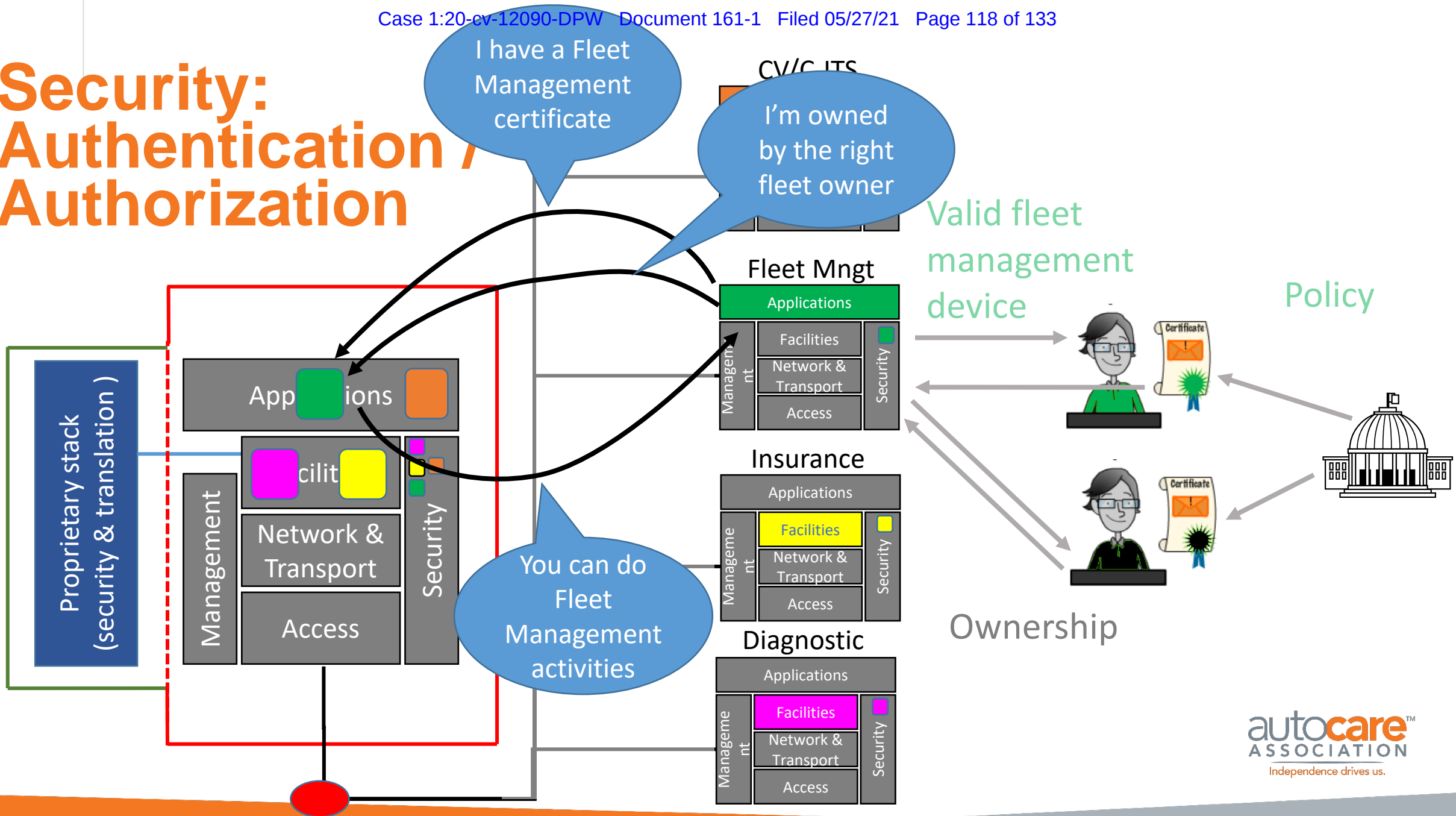
Security: Authentication / Authorization



Security: Authentication / Authorization

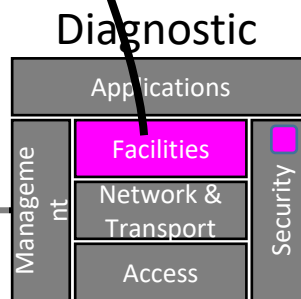
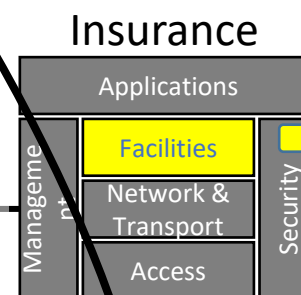
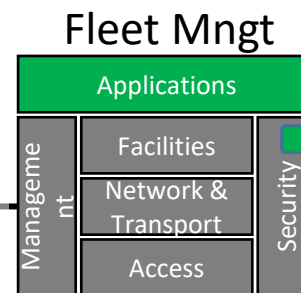
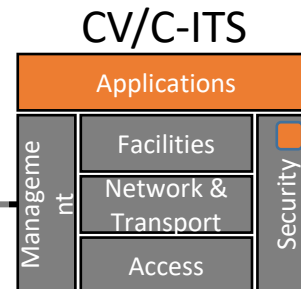
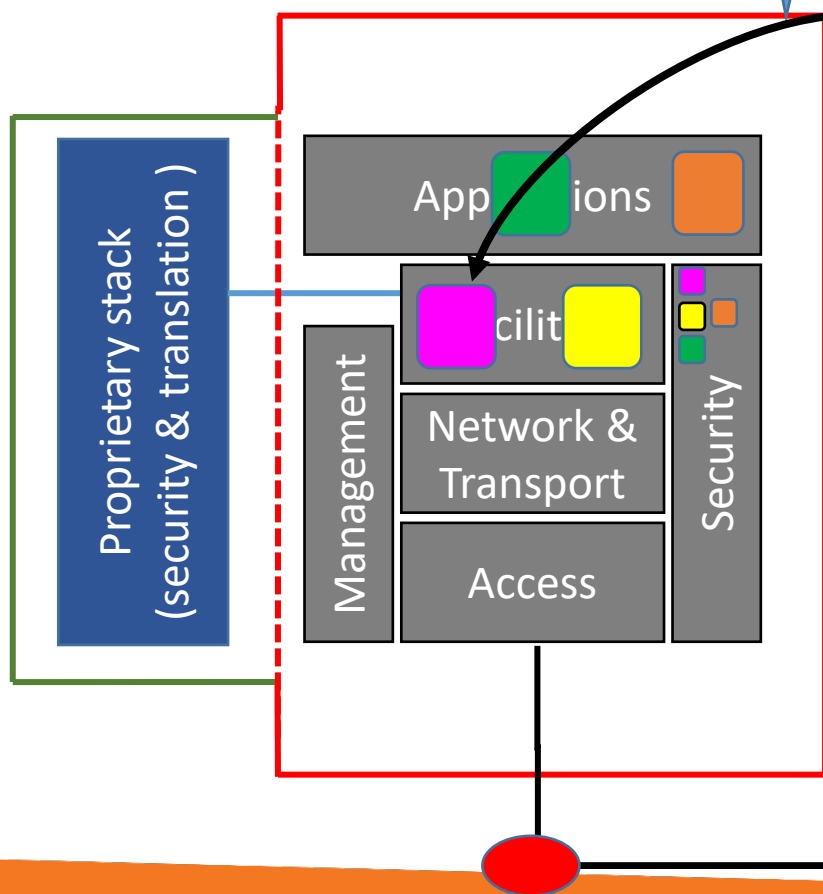


Security: Authentication / Authorization



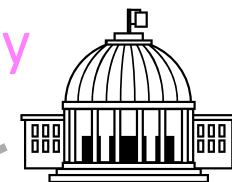
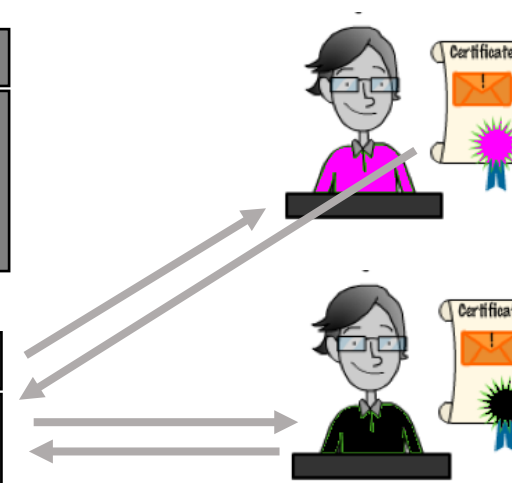
Security: Authentication Authorization

I have a
Diagnostics
certificate



Valid diagnostic
device

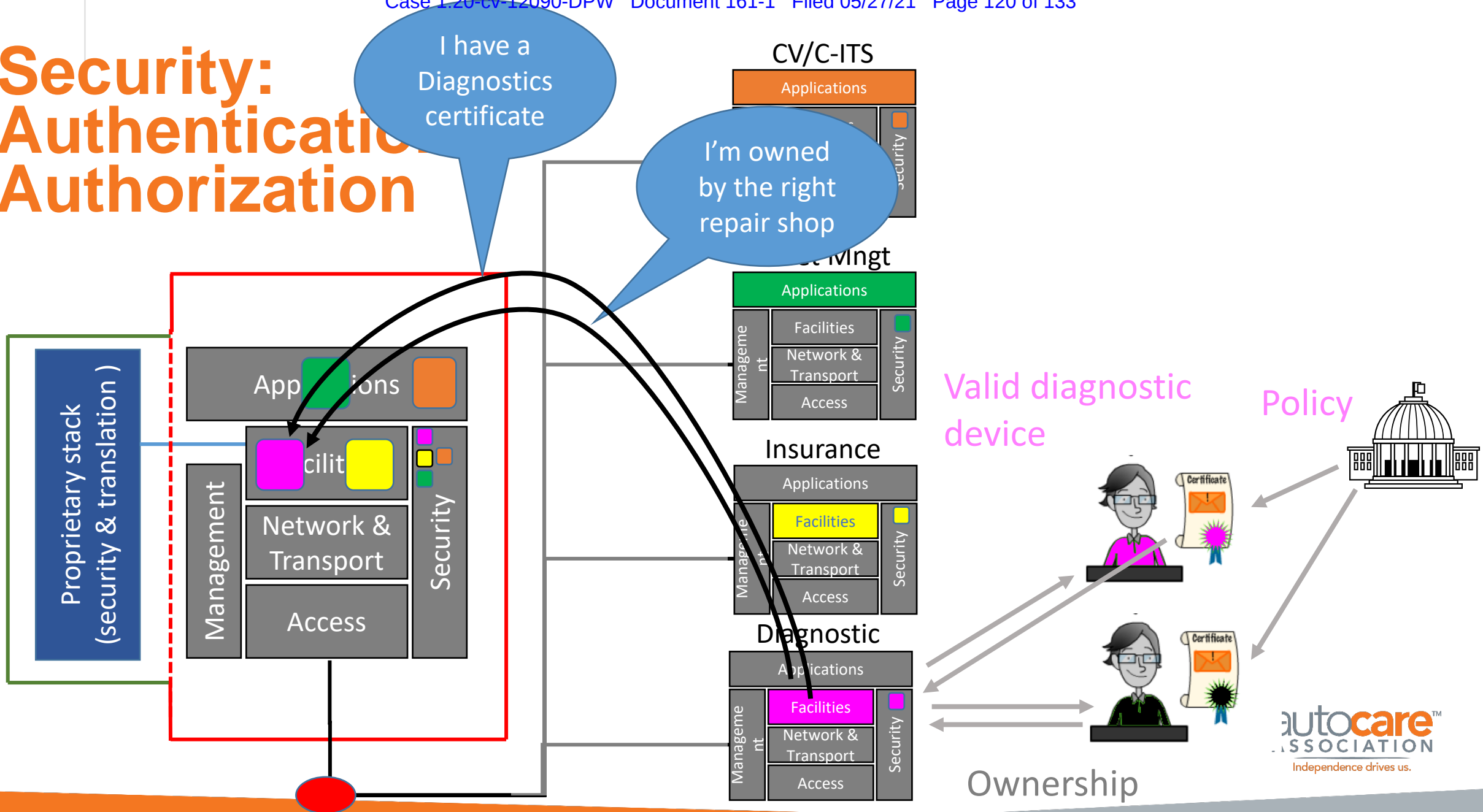
Policy



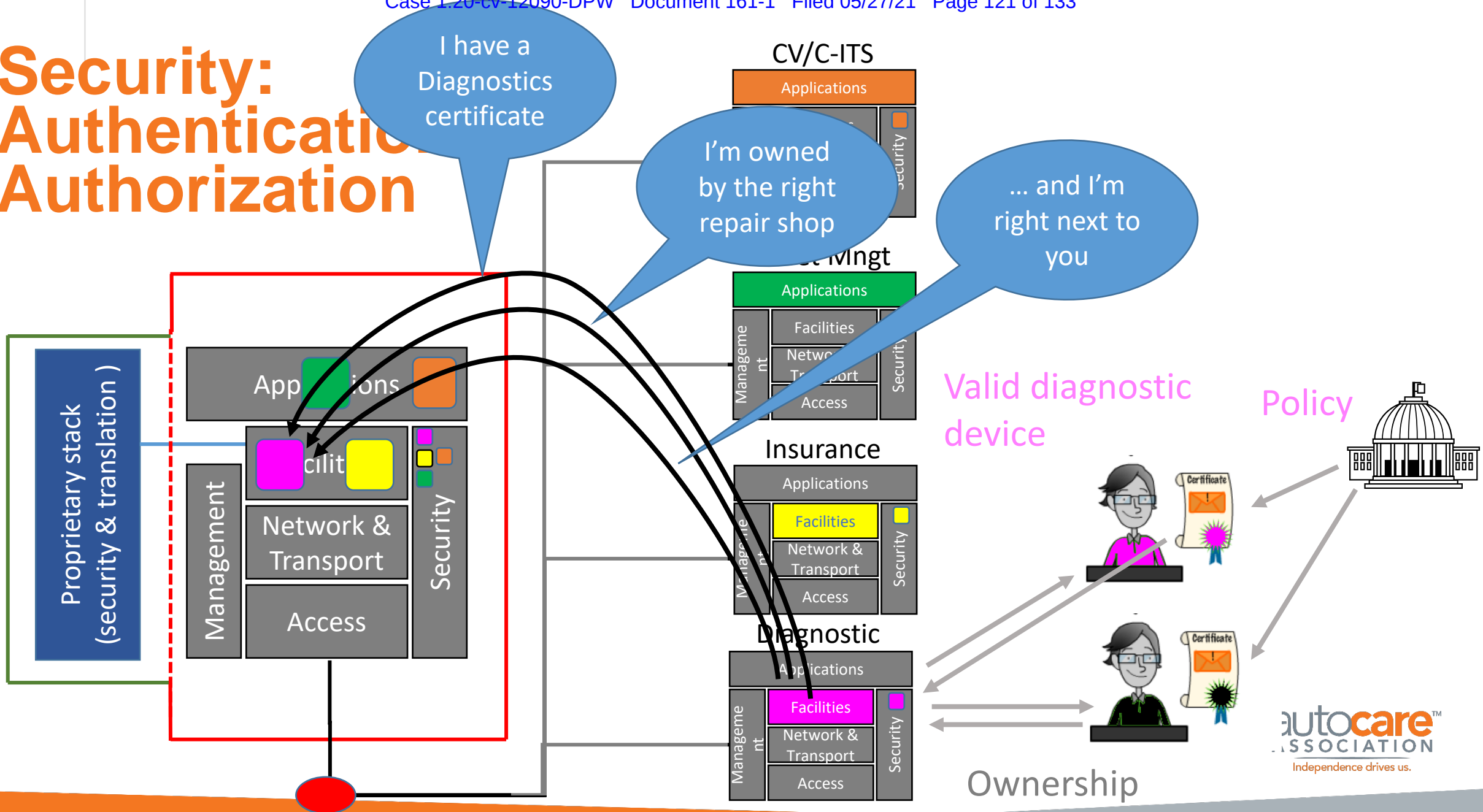
autocare[™]
ASSOCIATION
Independence drives us.

Ownership

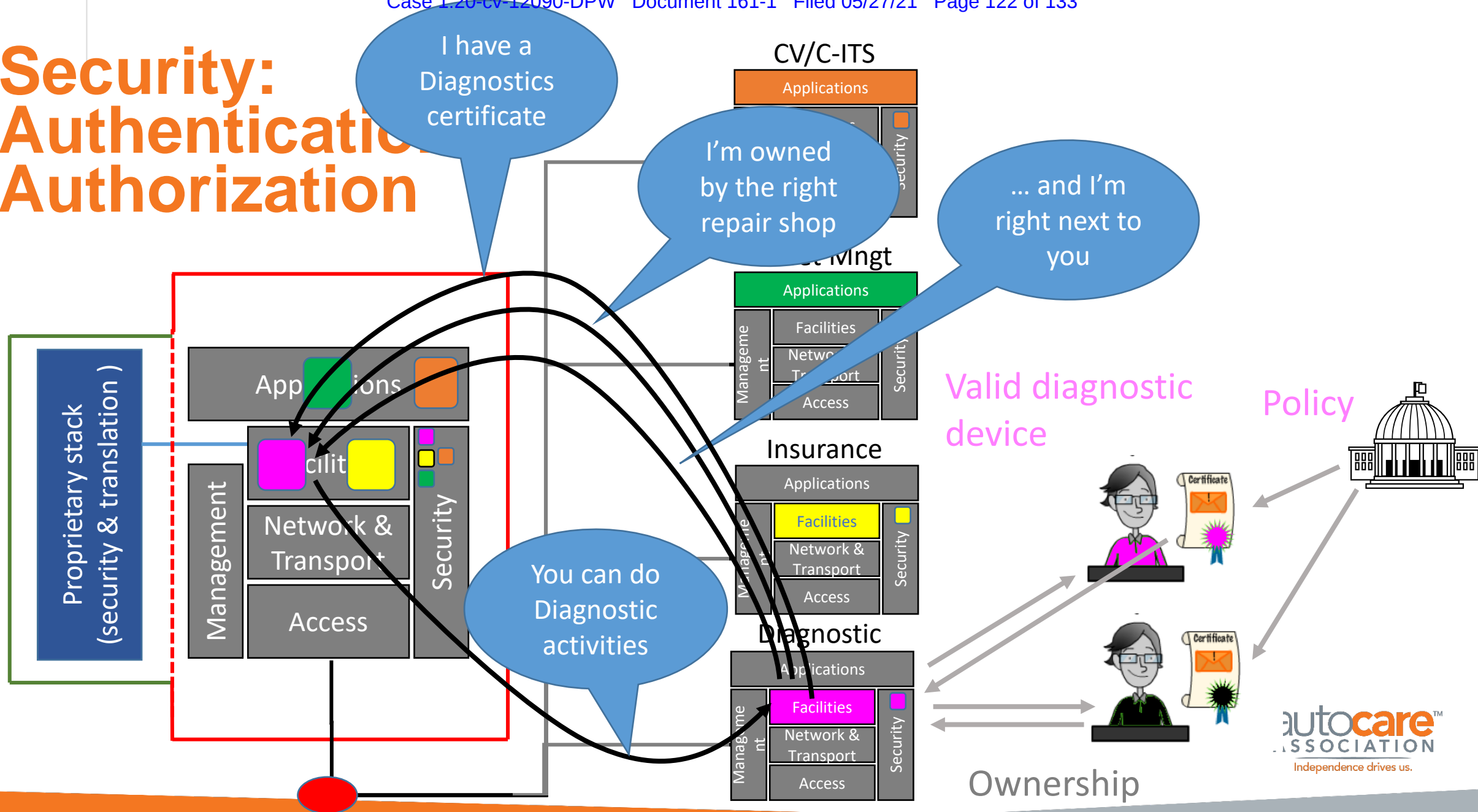
Security: Authentication Authorization



Security: Authentication Authorization



Security: Authentication Authorization



Current Activities

- Complete development of a full scale demo with multiple applications designed to address primary use cases
- Complete processes defining how certificates are issued in a trustworthy manner
 - How devices prove trustworthiness
 - Technical requirements
 - Certification processes
 - Governance processes for certification
 - How CAs get accredited
 - How to remove misbehaving CAs
 - Technically
 - Procedurally



Questions?

Exhibit 507



Mr. William Long
President and Chief Executive Officer
MEMA

Mr. Tim Musgrave
President & CEO, Pressure Systems Int'l
Pressure Systems International
Chairman, MEMA

Mr. Bill Hanvey
President and Chief Executive Officer
Auto Care Association

Mr. Mark Finestone
Executive Vice President, AutoZone, Inc.
Chairman, Auto Care Association

Mr. Ray Fisher
Executive Director
Automotive Service Association

Mr. Bob Wills
Owner, Wills Auto Service
President, Automotive Service Association

Mr. Paul McCarthy
President
Automotive Aftermarket Suppliers Association

Mr. Marc Blackman
CEO, Gold Eagle Company
Chairman, Automotive Aftermarket Suppliers
Association

Mr. Ray Pohlman
President
Coalition for Auto Repair Equality

Mr. Brian Plott
Executive Director
Engine and Tool Institute

Dear Friends and Colleagues:

We are living in unprecedented times as the U.S. economy struggles to cope with COVID 19. As we all continue to confront the challenges of this pandemic, we as an industry should consider how we might align our strengths and stand together to not only minimize the impact to our operations, employees, and customers, but also to find new opportunities to work together to prepare for the near-term and long-term transformations expected in our industry.

One of our top priorities during this crisis is to ensure that customers have access to a safe and well-functioning motor vehicle. In recent letters to President Trump and to each state's governor, we highlighted the critical importance of classifying vehicle repair and maintenance facilities as essential services. We strongly believe that these facilities, and the products and services they provide, are integral to helping communities and customers not only in times of need, but as part of a thriving automotive industry.

Looking beyond this immediate crisis, it is important to jointly consider the various aspects of uncertainty facing our industry. Our collective priorities should be obvious, and our efforts aligned. Of particular note are the concerns raised by the aftermarket supplier and independent repairer communities about access to diagnostic and repair data. For both sides to continue forward on this issue undaunted fails to consider the reality of our

new environment, post-COVID 19. To that end, our aspiration is to dedicate industry resources toward collaboration on this issue. As discussed recently with some of you, we would ask your associations to cease pursuit of the Massachusetts ballot initiative immediately, and any efforts underway in other states.

Accordingly, the Alliance for Automotive Innovation commits to a thoughtful dialogue about vehicle repair and diagnostic information including a sustained conversation about concerns from the aftermarket regarding access to this data.

We remain strongly committed to providing repairers everything they need to fully diagnose and repair vehicles while at the same time strongly opposed to the proposed ballot language in Massachusetts. Through such a dialogue, we are hopeful that we can each come to better understand our respective perspectives in order to find a path forward.

Our industries play a crucial role in protecting the safety of our customers and their vehicles. It is through the collaboration of ideas that we will be able to ensure that our nation's motor vehicle fleet remains as safe and operational as possible for generations to come. We respectfully request that you consider our proposal and respond back to us as soon as possible about your interest in an industry dialogue around access to vehicle data.

In the meantime, I hope you, your families and your colleagues remain healthy and safe.

Sincerely,

A handwritten signature in black ink, appearing to read "John Bozzella". The signature is stylized with a large, looped "J" and a cursive "Bozzella".

John Bozzella
President and CEO

Exhibit 508



May 19, 2020

Mr. John Bozzella
President and CEO
Alliance for Automotive Innovation
1050 K Street NW, Suite 650
Washington, DC 20001

Dear John,

Thank you for your letter regarding the Massachusetts ballot initiative. We agree that the industry must “align our strengths and stand together in order to minimize the negative impacts of COVID-19 and find new opportunities to work together to prepare for the near-term and long-term transformation expected in our industry.” We have been seeking this level of cooperation and open dialogue for the past several years and are pleased to know that the automakers are interested in reaching an agreement.

Over the past several years our associations have recognized the need for car owners to be aware of, and control access to, the data generated by their vehicles. In fact, our associations have reached out to your association as well as to individual manufacturers on several occasions over the last several years in an attempt to work cooperatively on a solution that will permit data being generated by vehicles to be securely available to shops where your customers want to have their vehicles serviced. Unfortunately, no progress has been accomplished from those attempts.

The Massachusetts Right to Repair Committee along with many of the groups copied on your letter will continue to pursue the ballot initiative in Massachusetts, however we all agree that a settlement prior to the July 1 deadline would be beneficial for all parties involved.

Per Massachusetts law, the Right to Repair Committee will not be able to withdraw the right to repair question from the November ballot after July 1. While a tight timeframe, we believe that the next month and a half provides an opportunity for both our industries to work together to reach an agreement that is in the best interest of U.S. vehicle owners. Although challenging, we want to emphasize that our side stands ready to meet as soon as possible to see if a solution can be reached.

Again, thank you for your letter and we look forward to working with the Alliance of Automotive Innovation to ensure that the motoring public has the knowledge and ability to control access to the repair data generated by today’s and tomorrow’s advanced vehicle systems.



Sincerely,

Mr. Bill Hanvey
President and CEO
Auto Care Association

Mr. Paul McCarthy
President
Automotive Aftermarket Suppliers Association

Mr. Ray Fisher
Executive Director
Automotive Service Association

Mr. Ray Pohlman
President
Coalition for Auto Repair Equality

Exhibit 510



7101 Wisconsin Avenue
Suite 1300
Bethesda, MD 20814
www.autocare.org

T: 301.654.6664
F: 301.654.3299
info@autocare.org

November 4, 2020

Mr. John Bozzella
President and CEO
Alliance for Automotive Innovation
1050 K St NW, Suite 650
Washington, DC 20001

Dear John,

Now that the November elections are over and the battle over the ballot question in Massachusetts is behind us, I am sure you agree that, based on the compliance deadline in the new law, it is critical that we move as soon as possible to begin the implementation of Question 1.

As you are no doubt aware, Auto Care has worked to share information with your staff and many of your members regarding a technology solution that can help ensure compliance with Question 1. This solution includes implementation of a collection of approved international standards that facilitate the safe and secure transmission of in-vehicle data. The standards include:

- ISO 21177 on cyber security
 - Security toolkit for access and session control.
- ISO 21184 on data management
 - Process for data registration, access and translation.
- ISO 21185 on communication profiles
 - Process how to standardize interfaces (OBD-II+, WiFi, 5G, etc).

As an option for compliance, use of these standards should permit your members to comply with requirements in Question 1 that mandate vehicle manufacturers "equip such vehicle with an interoperable, standardized and open access platform across all of the manufacturer's makes and models. Such platform shall be capable of securely communicating all mechanical data emanating directly from the motor vehicle via direct data connection to the platform."

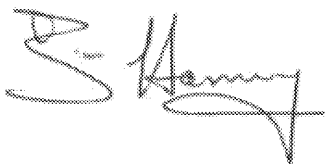
These standards also should ensure that manufacturers can implement requirements in Question 1 that "such platform shall be directly accessible by the owner of the vehicle through a mobile-based application and upon the authorization of the vehicle owner, all mechanical data shall be directly accessible by an independent repair facility or a class 1 dealer....."

The process for implementing these standards likely is assisted by the fact that some of your members are already implementing processes for securing access to vehicle data using similar techniques to those contained in the ISO standards. The difference being that under the current scenario, each manufacturer is utilizing a proprietary access protocol. However, Question 1 requires that "access to vehicle on-board diagnostic systems shall be standardized across all makes and models sold in the Commonwealth and is administered by an entity unaffiliated with a manufacturer." Moving to these ISO standards will simply move implementation to a standards-based approach which should benefit both our industries and ultimately both our customers.

Whether or not your members chose to use the ISO standards to comply, we believe that by setting aside the past battle and working together we can ensure an effective and timely implementation of the new law. In that spirit, I want to make our cyber security experts available to work with engineers from your member companies in order to ensure that they have the resources they need to meet the model year 2022 deadline.

Please let me know ASAP when you would like to set up a Webinar or conference call with our technical experts in order to provide additional information to your members. Also feel free to reach out to me should you have any questions or need any assistance as we move forward toward on this important initiative.

Sincerely,

A handwritten signature in black ink, appearing to read "W. Hanvey". The signature is stylized with a large, looped initial "W" and a cursive "Hanvey".

William Hanvey
President and CEO